Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

OPEN ACCESS Research Journal of Information Technology

ISSN 1815-7432
DOI: 10.3923/rjit.2017.46.63

Review Article
Inbuilt Image Encryption and Steganography Security Solutions for Wireless Systems: A Survey

Padmapriya Praveenkumar, K. Thenmozhi, John Bosco Balaguru Rayappan and Rengarajan Amirtharajan

School of Electrical and Electronics Engineering, SASTRA University, 613401 Thanjavur, India

Abstract

It is increasingly difficult to ensure the sharing of secret information due to uncontrolled technology explosion. In particular, the field of communication engineering has undergone a phenomenal innovation and expansion. At the same time disruptive innovation has grown significantly posing threats to all the positive innovations. On gaining information via wireless systems, intruders can get around firewalls and initiate denial of service over the networks and abuse the confidentiality of legal users. Strong encryption algorithms should be designed in order to protect the perceptive information that can be transmitted between wireless devices without interception. This has paved the way for extensive research in the field of information security to mainly detect and correct datum sabotage. In this context, development of wireless systems with inbuilt security layer can be an acceptable solution against any kind of disruptive innovation. Hence, this review study focuses on integrating schemes like OFDM, CDMA and MC-CDMA with steganography and image encryption techniques to develop wireless systems with inbuilt information security feature.

Key words: Image encryption, steganography, OFDM, CDMA, MC-CDMA

Citation: Padmapriya Praveenkumar, K. Thenmozhi, John Bosco Balaguru Rayappan and Rengarajan Amirtharajan, 2017. Inbuilt image encryption and steganography security solutions for wireless systems: A survey. Res. J. Inform. Technol., 9: 46-63.

Corresponding Author: Rengarajan Amirtharajan, School of Electrical and Electronics Engineering, SASTRA University, 613401 Thanjavur, India
Tel: +91 4362 264101 Fax: +91 4362 264120

Competing Interest: The authors have declared that no competing interest exists.

Data Availability: All relevant data are within the paper and its supporting information files.

INTRODUCTION

Wireless technology has witnessed a magnificent development in the recent decade and attained a stage where its non-existence will be felt by each and every individual of the universe. At the same time, this inevitable technology is at a crucial stage facing multidimensional cruel attacks from all quarters of computer made society[1]. In the process of developing various kinds of security solutions, both the creators and destroyers have been equally contributing to establish their strengths on wireless channels.

In the year 2013, over 31% of the phishing attacks were focused on financial institutions and out of this 225 attacks were carried out using fake bank[2]. In these attacks, hackers used trojan like viruses to abduct all the essential and holding information. On the other hand, the government of United States of America has reported the hacking of medical data of 4 million patients from Chicago medical group during the year 2013. In this attack, social security numbers and health information of patients stored in four unencrypted computers were stolen. Moreover, details of 780,000 patients from Utah Department of Health were hacked[3] during March-April 2012.

Tricare health centre at Virginia state lost the tapes which contained the health information of about 4,901,432 patients[4] in 2011. With reference to the recent survey made by Kaspersky, India is placed in the 6th vulnerable position facing frequent phishing attacks[5].

Also, it has reported that the websites of 22 government departments were hacked[1] in 2014. One of the leading security providers namely Rivest Shamir Adleman (RSA) has suggested that Indian corporate should develop comprehensive and dedicated information security systems to avoid different kinds of cipher attacks. Almost 35.4% of the phishing attacks were carried out on social networking websites especially on facebook and youtube.

In this context, development of wireless systems with inbuilt information security solutions have been proposed and implemented to plug the security holes as well as to curtail security breaches. The wireless systems considered are OFDM, CDMA and MC-CDMA schemes.

FREQUENCY DIVISION MULTIPLEXING TECHNIQUES

An overview: In order to tackle the intensifying demand for increased data rate and channel capacity of the transmission line, the multiplexing concept was introduced. The Frequency Division Multiplexing (FDM) technique was proposed to increase the bandwidth efficiency[6].

The FDM is a technique, where large number of simultaneous signal transmission is possible which helps in sharing of the bandwidth with minimum interference. It does not need any synchronization for its transmission and reception[7]. It supports full duplexing which is needed for most of our contemporary communication systems. However to accommodate and necessitate higher data rates in multimedia applications, Orthogonal Frequency Division Multiplexing (OFDM) has evolved[8].

The OFDM is a spectrally efficacious multichannel modulation scheme whose orthogonality has made it attractive over all modulation schemes. The orthogonality concept was first introduced by Chang[9] followed by Chang and Gibby[10] demonstrating the multiplexing in OFDM. The parallel transmission in OFDM was described by Saltzberg[11]. Zimmerman and Kirsch[12] have introduced higher data rates with effective spectral utilization in OFDM. Weinstein and Ebert[13] suggested data transmission through Discrete Fourier Transform (DFT) for orthogonality. Peled and Ruiz[14] introduced cyclic prefix to improve data transmission through frequency domain.

The escalating demand for high speed and noise free wireless communication systems were primitively tackled by the use of multiple access techniques like Frequency Division Multiple Access (FDMA), Code Division Multiple Access (CDMA) and Time Division Multiple Access (TDMA)[15]. The CDMA is one such technique which facilitates overlap of signal without interference and efficient use of bandwidth. The CDMA uses psuedo random noise (PN) sequences to modulate the data into wideband signal which is larger than minimum bandwidth required for the transmission of data[16].

Spreading of signal is accomplished by the use of PN codes which make the signal spread over the entire bandwidth and appears as noise to unintended users. The technique of modulating all the data onto same frequency band with different coding sequences is called Spread Spectrum (SS) technique[17]. In addition to SS technique, frequency hopping SS mechanism has also been used in CDMA system. In frequency hopping SS, carrier signal from the pool of frequency channels switches rapidly according to the PN sequence code[18].

The receiver with same coding sequence only can decipher the data, thus increasing the security. Also the cross correlation between any two codes is zero rendering them orthogonal. Hence, entropy and the orthogonality of the codes enhance the security multifold and lessen the interference. Thus the extensions of CDMA in communication technologies have yielded several advantages like greater capacity, improved security, privacy, rapid deployment, flexibility and asserting balance in phases of the signal.

Multi-Carrier CDMA (MC-CDMA) scheme couples CDMA and OFDM which provides strong and efficient frequency usage[19,20]. It has high spectral efficiency and facilitates the accommodation of more number of users than CDMA system. The MC-CDMA system couples the user specific PN sequence code that allows the data stream to be spread over the multiple sub carriers of CDMA and the orthogonality property of OFDM making it more robust in wireless domain[21,22].

In the current scenario, robustness is required in multipath environment, narrowband interference rejection, providing high capacity as well as in high speed broadband multimedia networks. These key features can be successfully met using OFDM, CDMA and MC-CDMA techniques to establish efficient wireless communication systems.

INFORMATION SECURITY

A perspective: The World Wide Web (WWW), cognized as the inspiration for technological evolution in the epoch of wireless communication has revolutionised the digital world by revivifying the data rates manifold. Coalesced with the evolution of internet, the number of users across the globe reached a huge number but simultaneously several methods of hacking also emerged. This in turn calls for higher data rate along with sound security. Over the decades, different kinds of information security techniques have been used to hide/embed/encrypt the critical data in various medium of communication, thereby guaranteeing the authenticity and confidentiality of the transmitted data[23]. Generally, security has been broadly classified based on application, computing, information, data and network as shown in Fig. 1.

In this classification, information security is further classified into steganography, cryptography and watermarking[23-25]. Steganography is basically transmitting secret information without the knowledge of others where as watermarking is known for copy right protection of the secret data to be transmitted[24].

Cryptography is the virtuosity of altering any information into a mode which is hard to make out for any common viewer except for the person handling it with the appropriate key. The data before performing this operation is called plain text and after the implementation is called cipher text. This is further grouped into two, namely symmetric key and asymmetric key cryptography[26]. The fundamental difference between the two types is that the former usually handles a shared key between the encryption and decryption sides, whereas the latter handles two keys namely private and public keys. Private keys are usually kept confidential and the public key will be known to the end users.

To deny the intruder the possibility of an existence of a message the modern technology employs a developed version of an age old technique called steganography. It is derived from the combination of Greek words steganos and graphein meaning concealed writing. It is the method of hiding information within information. The information can be text, image, audio or video files. Image is normally chosen as a cover object because of its redundancy, capacity and it supports almost all digital files[27].

Watermarking is mainly used for the purpose of authenticity and integrity. It is the process of embossing information on a carrier which is either related to it or not. This is done to prove the ownership of the information[28]. Watermarking is classified into fragile and robust. Fragile watermarking is the one as the name suggests is destroyed upon slightest modification. Robust watermarking can withstand any situation against it. This is again branched out into visible watermarking, invisible watermarking and fingerprinting.

Since, in this review, steganography and image encryption have been used to develop inbuilt information security wireless systems, they have been detailed in the following sections.

STEGANOGRAPHY

An overview: Steganography is a scientific art, where the secret message is shared to the receiver by hiding the same in a cover object, so that the very existence of the secret is

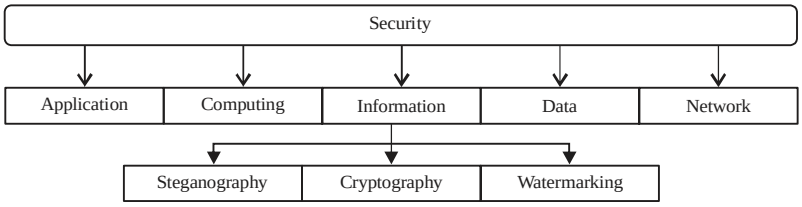

Fig. 1: Security classification

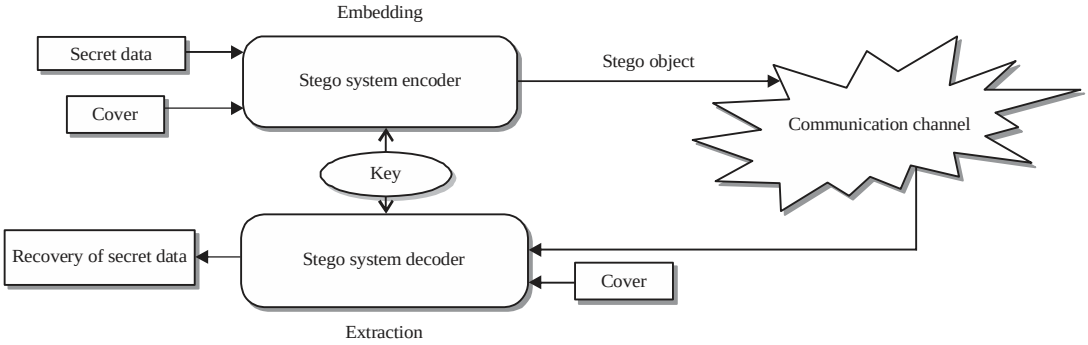

Fig. 2: Stego system

concealed. The first usage of stego was reported by Herodotus who was called as the father of steganography. He pointed out that in ancient Greek period the text was written on tablets and covered with wax. The other forms of secret hiding are[23,24]:

- Hiding the secret in the sole of shoes and in the ear rings of woman
- Secret message was written on wooden tables and then white washed and transmitted
- Pigeons to carry secret
- Micro dot method of hiding
- By varying the strokes and heights of the letters
- By using paper masks
- Gaspar Schott in his book "Schola steganographica" has explained the method of hiding using music notes
- Musicians could establish a covert channel and exchanging secret information on playing their music instruments as proposed by John Wilkins
- Secret data can be hidden between text using invisible ink

In steganography, the message to be transmitted is concealed in a multimedia file like image or audio or video called the cover image as depicted in Fig. 2.

Terminologies and requirements of stego system:

- **Key:** It is a numeric or alphanumeric or a symbol used for encryption and decryption that should provide security to any cryptographic algorithm
- **Cover:** It is a medium used for information hiding. It can be a text, video, audio and the most preferable format is the image
- **Stego object:** It is the object after embedding the secret data bits
- **Plain Text (PT):** Original information from the sender
- **Cipher Text (CT):** Using the cryptographic or encryption algorithm and the key, the PT will be converted into a non-readable format called as CT
- **Stream cipher:** It is the method of transforming PT into CT by applying the key and the stego algorithm to the data bit by bit
- **Block cipher:** It is the method of transforming PT into CT by applying the key and the stego algorithm to the data block by block
- **Pixel:** Pix (Picture) el(elements)/picture element or pixel is the smallest representation or illustration of any image. The intensity of every pixel in an image can be the same or different and is always a variable

The security of any crypto system lies in its key according to Kerchoff's principle[29]. The key is mainly classified into private and public key. Public key is the one which is known to the public and is used for embedding the secret data. Private key is the one which is used at the receiver end for the retrieval of secret data and often termed as secret key.

Requirements:

- **Robustness:** It is the withstanding capability of any stego algorithm that no suspicion should arise that covert communication has taken place
- **Imperceptibility:** Inability to distinguish between the original and the secret embedded image
- **Payload:** It is the ratio of secret bits to the cover image and it should be as high as possible

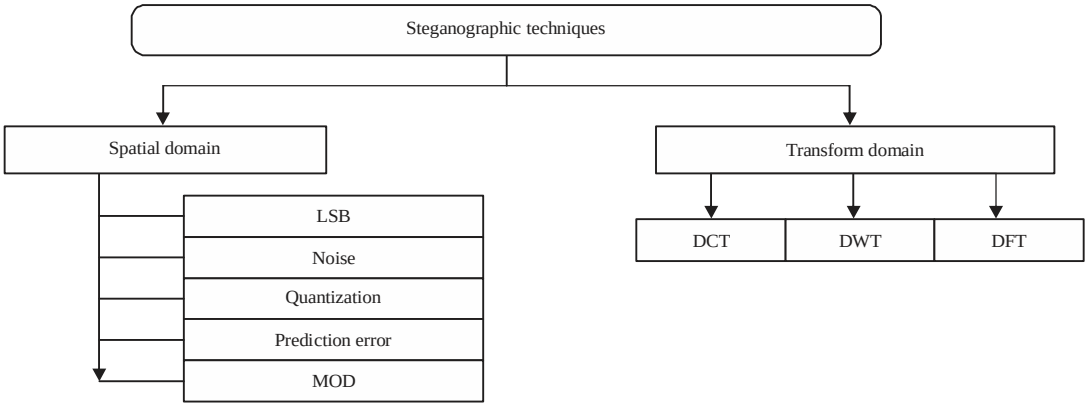

Fig. 3: Steganographic techniques

- **Method of embedding:** Based on the method of embedding there are various steganographic techniques available[27]
  - **Cover generation:** Here various covers are generated only for embedding the secret data bits
  - **Transform domain:** Hiding the secret data bits in the significant part of the cover image which will be done preferably in frequency domain
  - **Statistical method:** Here the cover object is modified in such a way to alter the statistical properties before embedding the secret data bits
  - **Distortion based:** In this method, the rearrangement or the layout of the cover has been modified for embedding the secret message
  - **Substitution:** Here the secret data will be embedded in the trivial part of the cover image
  - **Spread spectrum:** Here the secret data is multiplied by a PN sequence and then modulated before embedding in the cover object

Steganographic techniques: Science and technology redeem itself with its new creation and invention from time to time. The new expertise and knowledge not only facilitate us in new findings but also bring with it many new threats and security issues. So, to safe guard the information from all forms of unauthorized accesses and hacking, stego techniques are developed to carry out concealed or protected secret communication.

Image steganography is broadly classified into spatial and transform domain techniques as shown in Fig. 3. Spatial domain represents the direct manipulation or changes made in an image whereas transform domain is defined as the transformation of image into its frequency representation followed by modification on the spectral components of the image.

Spatial domain is further classified into Least Significant Bit (LSB), noise, quantization, prediction error and modulus techniques. In the LSB techniques, secret bits are embedded in the least significant bits of each pixel of an image. In this case the secret bits reflect the host bit without affecting the overall image quality. Noise based embedding refers to the process of hiding the secret data in the noisy pixels of an image. Quantization method of embedding is the process of applying quantization to the cover image and then secret data will be embedded. Prediction error method depends on the lossless compression procedure before embedding the secret data. Finally MOD based stego scheme refers to the method of applying MOD function to the cover pixels before embedding the secret data bits.

Transform domain is classified into Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT). In all the three cases, secret data are embedded on the coefficients of the transformed image. Frequency domain methods are more robust but compromise on payload and imperceptibility as compared with spatial domain techniques.

In spatial domain method, researchers have developed various schemes namely noise based embedding, quantization, prediction error and MOD etc. having LSB as the basis.

ENCRYPTION

An overview: Encryption arises from the Greek word "kryptos" which means secret. About 1500 BC, Assyrian merchants used a piece of stone called intaglio, in which they carved images for identification while doing transactions in trading. The enhanced digital version of this is termed as today's digital signature.

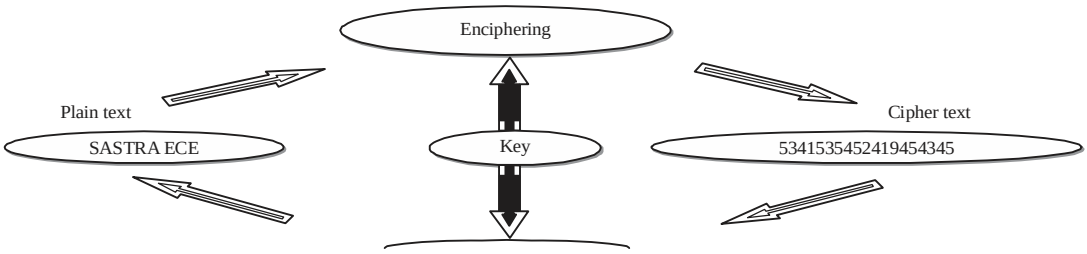

Fig. 4: Encryption model

Fig. 5: CIA triangle

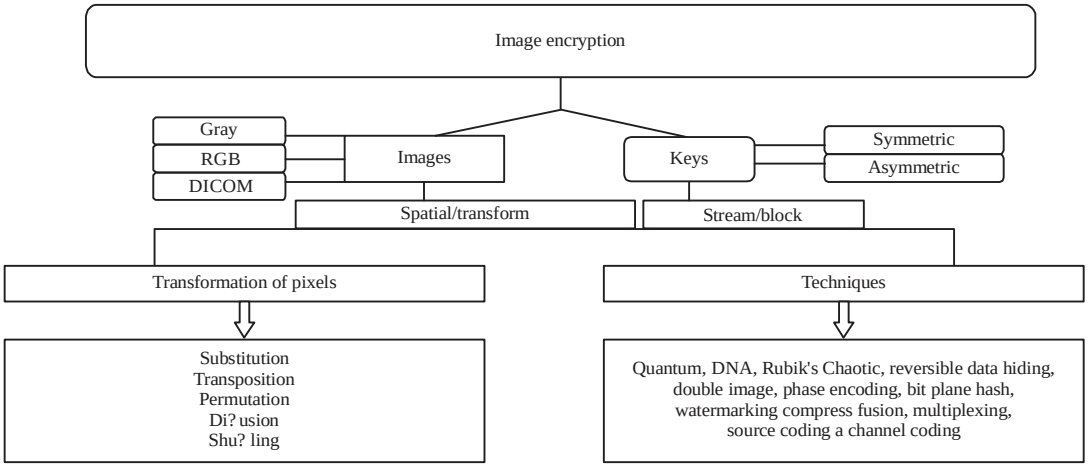

Fig. 6: Classification of image encryption

The necessities of any encryption algorithm should satisfy high capacity, redundancy and correlation among the pixels. The common technique that is used to secure the digital images is scrambling, so that original message of the image document should not be known and at the same time one could decrypt the original message with proper key[30].

Basically it is the process of transforming information using an algorithm or a method to make it unreadable to anyone except for those who have special knowledge regarding the transformed information. In this scheme, the characteristics of key play a vital role to decrypt the transformed image (Fig. 4).

Confidentiality, Integrity and Availability (CIA) are the three basic requirements that have to be accomplished by any encryption algorithm as given in CIA triangle (Fig. 5).

Image encryption has been broadly classified based on keys and types of images. Further, keys can be classified into either stream or block types. Similarly, images can be treated either on spatial or frequency domains. Figure 6 depicts the classification of image encryption techniques.

Based on the transformation of pixels in an image, there are numerous techniques available to produce cryptic effect[23]:

- **Shuffling:** It is the process of applying '1-1' mapping of the pixels in an image
- **Permutation:** It is the method of changing the order of the pixels in the image in a predetermined fashion
- **Rotation:** It is the angle of rotation made in the clockwise or anti clockwise sense in an image

- **Substitution:** It refers to the method of replacing the pixel values with a known data base
- **Product:** The process of performing substitution followed by transposition is termed as product
- **XOR:** Logical XOR will be carried out between PT and CT
- **Confusion:** It is the combination of substitution and permutation operations carried out between the CT and the key
- **Diffusion:** It is the combination of substitution and permutation operations carried out between the CT and the PT
- **Transposition:** It is the method of interchanging the row and column matrix of the given image pixels

Images are broadly classified into binary, colour (Red Green Blue (RGB) planes) and grayscale where an image is considered as an array of dots called as pixels and the number of pixels decides the size of an image:

- **Binary image:** It represents a kind of digital image, which has only two colours namely black and white. The black and white pixels are represented using single bit binary data (i.e.) 0 or 1
- **Grayscale image:** The grayscale image has many shades of gray colours where the darkest one is black and the lightest one is white. Each grayscale pixel can be represented by 8 bit binary data. The intensity of grayscale image varies from 0-255
- **Colour image:** It is one type of digital image which includes colour information of each pixel. Each pixel is represented by 3 bits planes namely RGB planes. Each plane is represented by 8 bits and therefore, 24 bits are required to represent each pixel

VARIOUS FILE FORMATS OF DIGITAL IMAGES

Digital Imaging and Communication in Medicine (DICOM): The DICOM is a standard for transmitting and storing medical images. National Electrical Manufacturers Association (NEMA) established the DICOM standard. It integrates printers, scanners, workstations, scan centers, doctor's premises and various medical instrument suppliers into a Picture Archiving Communication Systems (PACS).

Joint Photographic Experts Group (JPEG): It is a lossy image compression standard that was developed and accepted internationally from 1992. It operates in frequency domain and employs transform coding using Discrete Cosine Transform (DCT).

Tagged Image File Format (TIFF): It was created by Aldus Company, Washington in 1992. It is a file format used by computers for storing graphical images. It is widely supported by image manipulation applications.

Graphics Interchange Format (GIF): It supports Lempel-Ziv-Welch (LZW) lossless data compression technique which reduces the file size. It was introduced by CompuServe Company in the year 1987. It specifies the height, width and the display time of an image. It has been widely adopted by World Wide Web (WWW) interface.

Portable Networks Graphics (PNG): It was developed to provide better browser compatibility than GIF format. It adopts lossless compression scheme for storing, transmitting and displaying images.

Image encryption algorithm has been broadly classified based on the techniques such as quantum, hash function, RGB, grayscale, permutation, DNA, double image, bit plane, algorithm, chaotic, Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) and medical images.

Quantum based IE: The main advantage of using quantum based encryption is that once if the data has been encoded using quantum states and quantum key distribution it helps in detecting eavesdropping, while transmitting the secret data. In this technique, images are encrypted using quantum polarization states and their corresponding angles. Clarke *et al.*[31] proposed a method based on quantum digital signatures to transmit a message which cannot be forged and the security of the system was tested and analyzed by quantum mechanics. Abd El-Latif *et al.*[32] implemented quantum chaotic system providing substitution and diffusion operations in the ciphered output. Hua *et al.*[33] proposed a method based on image correlation decomposition for quantum gray-level encryption and decryption. Low computational complexity and resistance against various attacks were the advantages of this algorithm. Zaghloul *et al.*[34] suggested a quantum chaotic logistic map encryption procedure to generate key streams to generate different stages of ciphered output.

Hash function based IE: A hash function can be used to map digital data of varying size into an output of fixed size with negligible variations in input data and large variations in output data. Here, the input data is called as message and output data is called as message digest. Zuo and Cui[35] proposed an image hashing algorithm that was used to enhance the reliability and validity of image retrieval in the

encryption algorithm. Cheddad *et al.*[36] suggested 1D secure hash algorithm combined with a compound forward transform for encrypting digital images with password protection and steganography. Ahmed *et al.*[37] devised an image encryption algorithm providing authentication based on hash function. A hash based digital image encryption algorithm combined with self-adaptive scheme changed almost all the pixels in the cipher-image[38]. Hash based image encryption algorithms were mainly used in message authentication and digital signatures.

RGB based IE: While encrypting RGB images, the components were divided into red, green and blue components and then concatenated finally to produce the final encrypted image. Liu *et al.*[39] proposed a colour image encryption method based on cohen-grossberg neural network and proved to be an efficient algorithm with large key space. Wu[40] used fractional order hyper chaotic systems to provide highly secured encrypted color image. Kester *et al.*[41] proposed a hybrid encryption approach which uses RGB cryptographic technique and Advanced Encryption Standard (AES) algorithm to encrypt the images.

Grayscale based IE: Ahmad and Farooq[42] proposed an image encryption algorithm based on Multi-Level Block Scrambling (MLBS) which is highly sensitive and it has large key space. Chang and Hwang[43] proposed a method based on a phase modulation method in Fractional Fourier Transform (FrFT) domain and a Modified Gerchberg-Saxton Algorithm (MGSA) to limit the crosstalk in multi-plexing and multi-level encryption. Liu and Li[44] proposed a multi-plication of the pseudo vector on the pixel gray value of the digital image and based on the pseudo vector multi-plication and 2D Arnold transformation a digital image encryption algorithm has been introduced. Jin[45] proposed encryption based on Elementary Cellular Automata (ECA) with periodic boundary conditions. Zhou *et al.*[46] proposed a Parametric Switching Chaotic System (PSCS) based encryption system with their relative transforms. It combines various maps into a single system.

Permutation based IE: Liu and Li[44] proposed a digital image encryption algorithm based on the whole novel diffusion transformation and a three dimensional Arnold transformation to provide good diffusion properties and permutation. Liu and Sheridan[47] combines' image scrambling techniques with fractional Fourier transform to provide permuted image with a high key sensitivity. A two level bit permutation to provide secure image encryption scheme was introduced by Fu *et al.*[48]. Deng *et al.*[49] introduced image encryption algorithm based on permutation-diffusion structure and hyper chaotic system to provide secure crypto system.

Medical images based IE: Medical imaging is the approach of creating perceptible representation of internal structure clouded by bones and skins for medical attacks, clinical reasoning as well as to analyze disease. Mukherji[50] presented a novel method in telemedicine, where medical information was stored using smart card in an encrypted and compressed form. Sathishkumar *et al.*[51] presented a trusted medical image encryption method based on circular mapping using duo chaos. Dong *et al.*[52] proposed a zero watermarking algorithm using Discrete Cosine Transform (DCT) for medical images which eliminates the Region of Interest (ROI) selection to increase the speed of watermarking.

A joint watermarking and encryption system for protecting medical images using the combination of encryption, substitution watermarking and and quantized index modulation was proposed by Bouslimi *et al.*[53]. A pervasive mobile healthcare to access the medical data from wireless medium using Elliptical Curve Cryptography (ECC) algorithm with security was implemented by Sudha and Ganesan[54]. Huang *et al.*[55] presented an encrypted histogram equalized image for personal healthcare information which uses Advanced Encryption Standard (AES) algorithm for encrypting the images.

DNA based IE: A novel image encryption scheme employing Deoxyribo Nucleic Acid (DNA) sequence operations fused with chaotic system to resist various attacks was proposed. In this Coupled Map Lattice (CML) and DNA encoding rule were used to produce the scrambled output[56-58]. A more efficient bit level encryption based on DNA substitution and codon table was used to provide the diffused encrypted output[57]. Cryptography and steganography blended with DNA sequence has been proposed with 256 bits key to provide better security against intruders and hackers[57,58]. A three stage encryption was studied and implemented by Wang *et al.*[56], employing confusion, diffusion and transformation of pixels using DNA and Chebyshev's chaotic map. An evolutionary image encryption algorithm based on a hybrid model of DNA masking, Genetic Algorithm (GA) and a logistic map to provide improved DNA masks compatible with plain images was implemented[59]. A new image encryption algorithm using DNA and chaotic maps to alter the pixel values and its location were used to render encoding efficiency and to enhance the security of the cipher text.

Double Image based IE: Image encryption has been carried out in double images using gyrator transform and binary encoding procedure to provide highly encrypted cipher image[60]. Further, Shan *et al.*[61] proposed a double image encryption using chaotic maps and discrete multiple parameter fractional Fourier transform to provide scrambled output. An encryption scheme using Double Random Phase Encoding (DRPE) in the fractional Fourier domain and linear blend operation was presented by Wang *et al.*[62] and Sui *et al.*[63] proposed a double image encryption scheme where the encryption and decryption techniques used different keys to provide the ciphered matrix.

Shao *et al.*[64] proposed a double image encryption algorithm where double colour images were encrypted using quaternion gyrator domain into a single un-distinguishable image and generated encrypted images with various rotation angles. Chen *et al.*[65] presented a gyrator transform and local pixel scrambling technique for removing the cross-talk disturbance. Singh *et al.*[66] presented double phase images, where the images were phase masked and then transformed using gyrator transform in the frequency plane to provide secured encrypted output.

Chaotic based IE: Standard chaotic maps, Arnold maps, quantum chaotic sequences and tent maps were used to provide various encryption algorithms. Patidar *et al.*[67] proposed a permutation-substitution method for image encryption using chaotic standard map. He *et al.*[68] proposed an encryption algorithm adopting scrambling of Arnold chaotic sequences to provide diffused encrypted image. Zhu *et al.*[69] proposed a method based on chaos using the principle of magic cube transformation and pseudorandom sequences to provide highly efficient encrypted output rendering large key space. Ye and Zhou[70] presented a chaotic image encryption method which involves two dimensional tent map with two control parameters for providing encrypted diffused output.

Bhatnagar and Wu[71] proposed an image encryption method adopting saw tooth space filling curve and pixel of interest method to scramble and select the pixel to provide transformed encrypted output. Ye[72] proposed an image encryption method based on chaos with permutation diffusion concept involved with six dimensional Arnold map and skew tent maps to resist against various attacks.

Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) based IE: Ke *et al.*[73] presented a novel watermarking method in DWT domain using chaotic encryption. Logistic chaotic sequence and DWT were used to shuffle the watermark to provide copy right protection in the encrypted image[74]. The DWT based watermark bits for selecting the position of embedding the watermarks in an encrypted image was proposed by Keyvanpour and Merrikh-Bayat[75]. Elshazly *et al.*[76] proposed a watermarking algorithm in DWT domain based on mean quantization and chaotic sequences to provide encrypted output.

Out of the various image encryption schemes discussed in the survey, few image encryption schemes has been analyzed and implemented to provide transposition, shuffling, substitution, permutation and diffusion of the encrypted image. The images considered are grayscale, RGB and DICOM, respectively. Firstly, in key based encryption, a rapid key encryption procedure employing symmetric key adopting matrix array using grayscale image was developed[77]. A complex and multi-layered key generation scheme employing pseudo-random sequence, discrete cosine transform, quantization and scrambling was adapted. The operations like diffusion and substitutions were inherently inducted into the proposed scheme to provide faster convergence of cipher image. Secondly, a tri-layer encryption scheme has been proposed and uses RGB image, where a combination of space filling curve with chaos has been used for encryption process. Initially three chaotic sequences were generated using Chua's equations followed by quantification of those sequences[78]. Hilbert curve based key was used for image scrambling. Finally, Gould transform was applied to enhance image authentication and tamper proofing of the encrypted image. In addition, DNA based complementary addition rule was integrated to make the proposed scheme robust against statistical attacks.

Yet another tri-layer cryptic solution has been implemented on Digital Imaging in Communication and Medicine (DICOM) images to establish secured communication for effective referrals among peers without compromising the privacy of patients[79]. In this approach, a blend of three cryptic schemes, namely Latin Square Image Cipher (LSIC), Discrete Gould Transform (DGT) and Rubik's encryption have been employed. Among them, LSIC provides better substitution, confusion and shuffling of the image blocks, DGT incorporates tamper proofing with authentication and Rubik renders a permutation of DICOM image pixels. The developed algorithm was also implemented in Universal Software Radio Peripheral (USRP) environment using the Additive White Gaussian Noise (AWGN) channel model and the attack analysis was performed by introducing random cropping.

Information security for wireless systems: Wireless communication is one of the demanding and challenging technologies from time to time[80]. The exponential growth of multimedia over internet makes inevitable to digitize the data to be published, transmitted and shared on internet[81]. The evolution of new products and services emerging on almost daily basis demands for higher data rate. With the evolution of internet, the number of users across globe reached a huge number but simultaneously several methods of hacking also increased. This in turn calls for higher data rate along with sound security features.

Stego integrated OFDM: To enhance the security feature of OFDM systems, various researchers encompass stego based algorithms to ensure integrity and authenticity. Dual field OFDM based chaotic encryption has been addressed by various algorithms to Wang *et al.*[82], Quyen *et al.*[83] and Xiao *et al.*[84] ensure large key space, feasibility and security.

The orthogonal subcarriers in OFDM are interleaved according to the dynamic channel state information available to the transmitter provides permuted data which in-turn fails the eaves droppers resilience attacks by providing maximum reliable transmission[85]. During transmission, appending Cyclic Prefix (CP) greater than or equal to the channel order is primarily used to avoid Inter block interference (IBI). Then the size of the CP in each OFDM symbol is varied pseudo-randomly to suppress the cyclo-stationary features ensuring secured OFDM waveform. For secure and robust transmission of OFDM signals, symmetric key based cryptographic algorithm has been proposed by Al-Dweik *et al.*[86] and secret key sharing has been carried out using Low Density Parity Check codes (LDPC) and constellation mapping[87] to resist against intruders.

To enhance transmission in OFDM system, cooperative relay selection based on subcarriers has been carried out leading to different achievable rates over each subcarrier with enhanced security[88]. Sun *et al.*[85] proposed a covert communication for OFDM system using cyclic delay diversity raising tremendous security concerns. A physical layer security review on OFDM has been addressed in the presence of noise, interference, multipath fading and jamming attacks and includes WiMAX and Long Term Evolution (LTE) standards. The main disadvantage with OFDM is the high Peak Average to Power Ratio (PAPR), which can be eliminated by multi phase orthogonal matrix family as a key to guarantee data security and reduced PAPR[89].

Stego integrated CDMA and MC-CDMA: Marvel *et al.*[90] introduced Spread Spectrum Image Steganography (SSIS) where secret data were hidden and recovered using appropriate keys generated using spread spectrum technique without the knowledge of original image. Cox *et al.*[91] proposed a secure tamper resistant algorithm with spread spectrum technique for digital watermarking to provide robust and strong resilience against collision attacks. Chaos based SSIS (CSSIS) has been implemented using chaotic encryption and modulation schemes to provide authentication and tamper proofing in covert communication[92]. Chandramouli and Subbalakshmi[93] proposed two active steganalysis schemes for SSIS to extract the hidden secret data bits. The audio data in steganography using DSSS scheme has been implemented by Nugraha[94]. Here the data must be modulated using the pseudo-noise and then embedding was carried out to provide a robust steganographic scheme[95]. The benefits of spread spectrum technique together with error-correcting code combined with DFT to increase the robustness of the system were proposed by Youail *et al.*[96]. The aesthetic appeal of CDMA and steganography together has revolutionized the present world communication systems. Entropy criterion with CDMA using digital watermarking in Discrete Wavelet Transform (DWT) has been carried out to ensure attack free transmission and reception. Authentication and key agreement protocols has been used[97] to provide user confidentiality and to defy against various attacks like redirection attacks, man in the-middle attack, sequence number depletion attacks and roaming attacks.

Chaos incorporated DS-CDMA has been carried over in presence of AWGN and multipath environments to provide higher security then the conventional CDMA systems. For good cross correlation properties and improving quality of security, orthogonal coding CDMA has been introduced by Mushtaq *et al.*[98]. The MC-CDMA system is robust to frequency selective fading and provides efficient frequency usage. It has high spectral efficiency and facilitates the accommodation of more number of users than CDMA system. The MC-CDMA uses specific PN sequence code that allows the data stream to be spread over the multiple sub carriers. It is used to improve security, data transmission rate and to minimize Inter Symbol Interference (ISI)[99].

To counteract these security issues, IEEE 802.11 introduced encryption and authentication methods[100]. But the security measures introduced were flawed because of the weaknesses in the key length, key management and could not sustain mutual authentication leading to serious security issues.

Hacking and intrusion are the two disruptive techniques challenging all the advantages of wireless technology. In this context, development of wireless systems with inbuilt security layer can be an acceptable solution against any kind of disruptive innovation. This study focuses on integrating

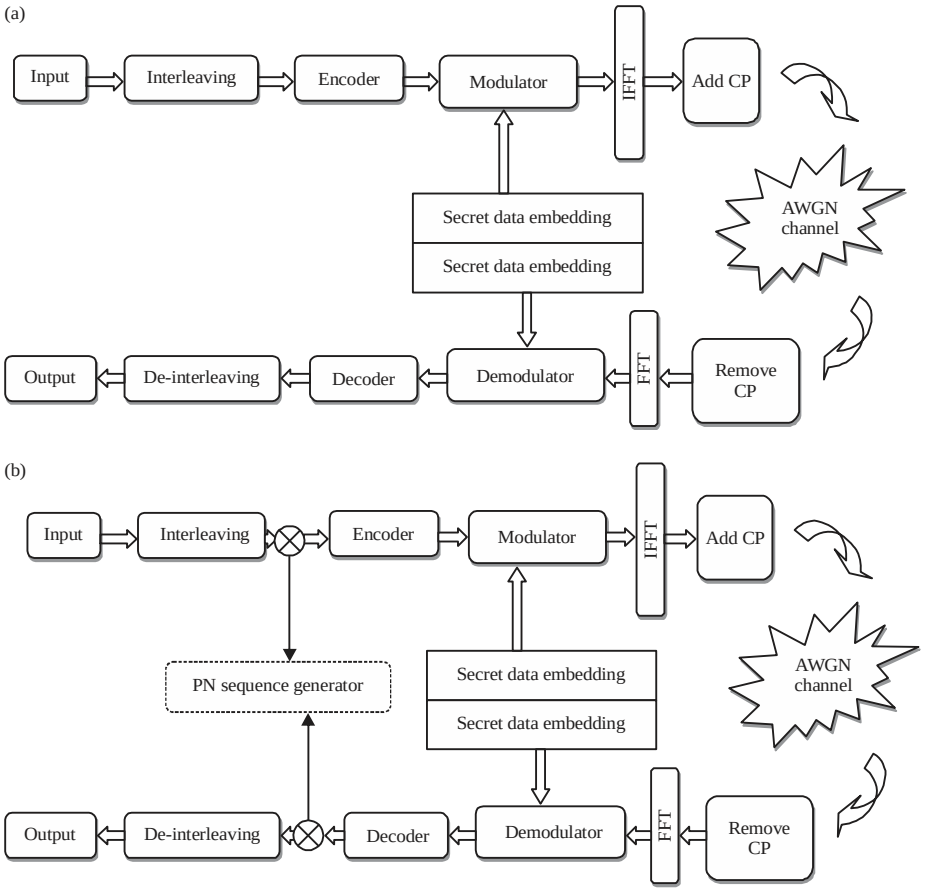

Fig. 7(a-b): Stego integrated (a) OFDM model and (b) MC-CDMA model

schemes like OFDM, CDMA and MC-CDMA with steganography and image encryption techniques to develop wireless systems with inbuilt information security feature. In steganography techniques, LSB and SSIS were adopted and developed to increase the imperceptibility of the hidden message.

With the motivation of developing wireless systems with inbuilt security layer, phase components of the modulation schemes employed in OFDM and MC-CDMA systems[101] have been used to hide secret data without affecting the overall quality of communication as shown in Fig. 7a and b, respectively[102-104]. In this implementation, various types of interleavers and error control codes like convolutional encoders, RS codes, turbo codes of various rates like 1/2, 1/3, 2/3, 3/4 etc. have been used and .integrated with the wireless systems to overcome the burst and random errors. Further, various digital modulation schemes namely BPSK, QPSK and QAM were used to accommodate different data rates[102-104].

The integration of steganography and chaos based image encryption algorithms with OFDM have been accomplished to maintain integrity and confidentiality of the data transmitted over wireless system[103]. Th eBER and correlation values were computed to prove the robustness of the system.

Performance evaluation metrics: To analyze the performance of steganographic and image encryption integrated OFDM, CDMA and MC-CDMA systems, various metrics namely correlation coefficient, NPCR, UACI, entropy and BER were computed. Among them, BER and E_b/N_o are the key parameters to assess the performance of the wireless systems while transmission under any source of noise or interference or adverse channel conditions.

Bit Error Rate (BER): The BER is defined as the number of bit errors occurred to the total bits transmitted over the channel[105]. It can also be defined in terms of probability of error (P_e) which is always proportional to E_b/N_o and it represents the SNR. The E_b is defined as the ratio of carrier power to the bit rate and N_o represents the noise power spectral density. The BER will be affected by interference, higher transmitter power, lower order modulation and bandwidth.

Correlation of pixels: To analyse the performance of the encryption algorithms, correlation of the pixel values for the considered image prior and post cryptic operations was computed. Horizontal (HC), vertical (VC) and diagonal (DC) correlation values of the encrypted images were computed. Generally, the correlation value of one indicates high correlation and zero points to obscurity among the pixels. The image encryption standards are necessitated to provide zero correlation values. Two adjacent pixels for vertical, horizontal and diagonal directions were selected and the correlation coefficients (r_{xy}) were calculated[106-108]:

$$r_{xy} = \frac{COV(x, y)}{\sqrt{D(x)}\ \sqrt{D(y)}}$$

Where:

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - \frac{1}{N}\sum_{i=1}^{N}x_i\right)^2$$

$$D(y) = \frac{1}{N}\sum_{j=1}^{N}\left(y_j - \frac{1}{N}\sum_{j=1}^{N}y_j\right)^2$$

$$COV\ (x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - (E(x))(y_i - (E(y))$$

where, N denotes the possible pairs of pixels and x, y represents the adjacent pixels in the image. The E(z) is the expectation operator and is given by:

$$E(z) = \frac{1}{N}\sum_{i=1}^{N}z_i$$

Entropy analysis: Entropy determines the uncertainty in the final encrypted image and is given by:

$$Entropy = \sum_{j=1}^{m}(p(y_j)\log_2 1/p\ (y_j)$$

where, m denotes the grayscale values of the image and p(y) represents the pixel value from the histogram of the encrypted image. The value of this entropy should be close to 8 for greyscale image to prove the robustness of the algorithm[109-111].

Differential attacks: Differential attacks were performed to analyse the strength and endurance level of the proposed algorithm. This technique was implemented by observing one pixel in the plain image and the corresponding change in the resultant image. If the change is evident in the resultant image, then it is asserted that the attack is rendered useless. There are two major constraints of differential attacks, namely Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI)[112,113].

NPCR: It is the evaluation between two images by considering the corresponding pixel values with dissimilar grey levels. If $P_1(x, y)$ and $P_2(x, y)$ are the pixel grey level values in the xth row and yth column of the image M×N respectively, where M and N represents the row and column of the image[114,115]:

$$NPCR(\%) = \frac{\sum_{x, y}Q(x, y)}{M \times N} \times 100$$

Then:

$$Q(x, y) = \begin{cases} 0 \text{ if } p_1(x, y) = P_2(x, y) \\ 1 \text{ if } p_1(x, y) \neq P_2(x, y) \end{cases}$$

UACI: It is defined as the average intensity difference between the pixels in grey level for the two images. If $P_1(x, y)$ and $P_2(x, y)$ are the pixel grey level values in the xth row and yth column of the image M×N, respectively, where M and N represents the row and column of the image[116,117]. Then UACI is given by:

$$UACI = \frac{1}{M \times N}\left[\sum_{x, y}\frac{p_1(x, y) - p_2(x, y)}{2^{graylevel} - 1}\right]$$

Histogram tests: Histogram is a graphical illustration of the pixel data of an image and was introduced by Karl Pearson. It is the representation of variation in the perception of a colour also known as tone. The x-axis represents the tonal variations of the image and the y-axis represents the number of pixels of a particular tone. The original cameraman image is shown in Fig. 8a and its histogram is shown in Fig. 8b, which shows the pixel distribution and its variation[118,119]. To prove the sternness of the encryption schemes, cropping and noise attacks were carried out.

Cropping attacks: Cropping is intentionally deleting some pixel values in the encrypted image and passing it over the decryption algorithm. Then the decrypted image can be analyzed to test the robustness of the encryption scheme adopted[120].

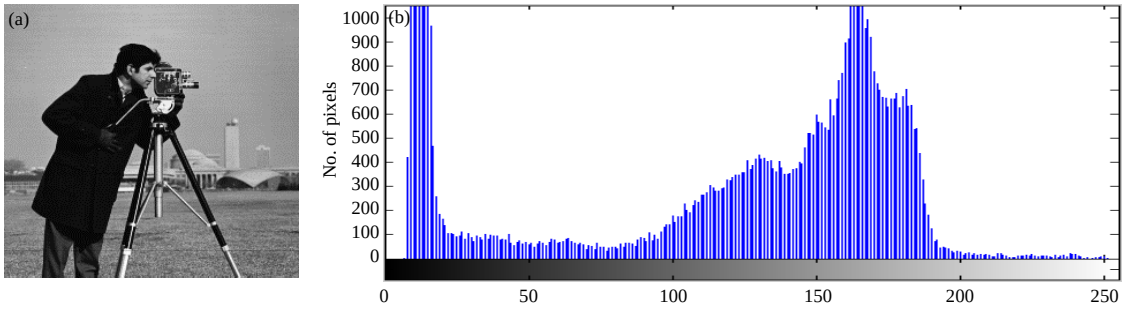

Fig. 8(a-b): (a) Original cameraman image and (b) Histogram of original cameraman image

Key sensitivity: It represents the sensitivity of the encryption algorithm when a wrong key is used to decrypt the original image. The secret key employed should be extremely sensitive and even if a slight variation occurred in the key then the decryption algorithm should provide a completely obscured image. For an ideal case, the sensitivity of the secret key should be as large as possible[121].

Key space: Key space represents the total combinations of distinct keys which can be used in any encryption and decryption algorithms. It is an important parameter to measure the robustness and sternness of the proposed encryption scheme against various attacks. Larger the key space, greater the probability of reducing the threat of an attack. Key space is one of the factors that control the feasibility of any exhaustive key search attack to find the secret key. It should be large enough to make any brute force attack impossible[106,110,112-125].

CONCLUSION

In this literature survey, various steganographic and image encryption schemes with their merits and demerits have been highlighted. Further the enhancement of security features of wireless systems were discussed to provide inherent secured wireless systems (OFDM, CDMA and MC-CDMA) using stego and image encryption based schemes. Based on the survey, the importance of integrating security techniques in wireless systems has been strongly felt and motivated to carry out this survey work. The effectiveness of the stego and IE schemes was estimated through BER, correlation values, NPCR and UACI. Performance analysis indicated that the BPSK and QAM provides better BER and data rate as compared to other modulation schemes, respectively. The methods were tested using hardware and software platforms. Tested in AWGN channel attacks and cropping attacks to validate the robustness of the proposed schemes. From the survey, stego integrated OFDM with convolution encoder 2/3 and OFDM with chaos based image encryption proves to be the better schemes. Wireless technologies blended with information security emerged as a solution for all types' communication threats and problems.

SIGNIFICANCE STATEMENTS

- Development of wireless systems with inbuilt information security feature
- Wireless systems like OFDM, CDMA and MC-CDMA were considered
- Steganography and image encryption algorithms were integrated with wireless systems
- Metrics like BER, NPCR, UACI, entropy, correlation of pixels and histogram tests were discussed
- Stego integrated CDMA, OFDM and MC-CDMA were analyzed

REFERENCES

1. The Economic Times, 2014. India 6th most frequently phishing attacked nation: Kaspersky. April 11, 2014. http://economictimes.indiatimes.com/tech/internet/india-6th-most-frequently-phishing-attacked-nation-kaspersky/articleshow/33621016.cms?intenttarget=no
2. The Economic Times, 2014. Information stealing virus detected in online banking space. Januray 20, 2014. http://articles.economictimes.indiatimes.com/2014-01-20/news/46374631_1_pos-malware-virus
3. Kitten, T., 2013. FBI warns of spear-phishing attacks. July 2, 2013. http://www.bankinfosecurity.com/fbi-warns-spear-phishing- attacks-a-5878/op-1
4. BGR Media, 2014. Cyber criminals imitate FIFA website for phishing: Kaspersky. July 10, 2014. http://www.bgr.in/news/cyber-criminals-imitate-fifa-website-for-phishing-kaspersky/
5. Krebs on Security, 2015. Hacked hotel phones fueled bank phishing scams. February 4, 2015. https://krebsonsecurity.com/2015/02/hacked-hotel-phones-fueled-bank-phishing-scams/

6. Bingham, J.A.C., 1990. Multicarrier modulation for data transmission: An idea whose time has come. IEEE Commun. Mag., 28: 5-14.
7. Rappaport, T.S., 2002. Wireless Communications: Principles and Practice. 2nd Edn., Prentice Hall, UK., ISBN: 0130422320.
8. Cimini, L.J., 1985. Analysis and simulation of a digital mobile channel using orthogonal frequency division multiplexing. IEEE Trans. Commun., 33: 665-675.
9. Chang, R.W., 1970. Orthogonal frequency division multiplexing. U.S. Patent No. 3488445.
10. Chang, R. and R. Gibby, 1968. A theoretical study of performance of an orthogonal multiplexing data transmission scheme. IEEE Trans. Commun. Technol., 16: 529-540.
11. Saltzberg, B., 1967. Performance of an efficient parallel data transmission system. IEEE Trans. Commun. Technol., 15: 805-811.
12. Zimmerman, M. and A. Kirsch, 1967. The AN/GSC-10 (KATHRYN) variable rate data modem for HF radio. IEEE Trans. Commun. Technol., 15: 197-204.
13. Weinstein, S. and P. Ebert, 1971. Data transmission by frequency-division multiplexing using the discrete fourier transform. IEEE. Trans. Commun., 19: 628-634.
14. Peled, A. and A. Ruiz, 1980. Frequency domain data transmission using reduced computational complexity algorithms. Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, April 19-24, 1980, Taipei, Taiwan, pp: 964-967.
15. Lee, J.S. and L.E. Miller, 1998. CDMA Systems Engineering Handbook. Artech House, London, ISBN: 9780890069905, Pages: 1228.
16. Hara, S. and R. Prasad, 1999. Design and performance of multicarrier CDMA system in frequency-selective Rayleigh fading channels. IEEE Trans. Vehic. Technol., 48: 1584-1595.
17. Liberti, Jr. J.C. and T.S. Rappaport, 1999. Smart Antennas for Wireless Communications, IS-95 and 3G CDMA Applications. Prentice Hall, New Jersey, USA.
18. Chouly, A., A. Brajal and S. Jourdan, 1993. Orthogonal multicarrier techniques applied to direct sequence spread spectrum CDMA systems. Proceedings of the Global Telecommunications Conference, November 29-December 2, 1993, Houston, TX., USA., pp: 1723-1728.
19. Hara, S. and R. Prasad, 1997. Overview of multicarrier CDMA. IEEE Commun. Magaz., 35: 126-133.
20. Hara, S. and R. Prasad, 1996. DS-CDMA, MC-CDMA and MT-CDMA for mobile multi-media communications. Proceedings of the IEEE 46th Vehicular Technology Conference on Mobile Technology for the Human Race, Volume 2, 28 April-1 May, 1996, Atlanta, GA., pp: 1106-1110.
21. Hanzo, L. and T. Keller, 2006. OFDM and MC-CDMA: A Primer. Wiley, New York.
22. Hanzo, L.L., M. Munster, B. Choi and T. Keller, 2005. OFDM and MC-CDMA for Broadband Multi-user Communications, WLANs and Broadcasting. John Wiley and Sons, New York, USA.
23. Stefan, K. and A. Fabin, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, London, UK.
24. Cheddad, A., J. Condell, K. Curran and P. McKevitt, 2010. A hash-based image encryption algorithm. Opt. Commun., 283: 879-893.
25. Stallings, W., 2006. Cryptography and Network Security: Principles and Practice. 4th Edn., Prentice Hall, New Jersey, ISBN: 0130914290.
26. Petitcolas, F.A.P., R.J. Anderson and M.G. Kuhn, 1999. Information hiding-a survey. Proc. IEEE, 87: 1062-1078.
27. Menezes, A., P. van Oorschot and S. Vanstone, 1996. Handbook of Applied Cryptography. 1st Edn., CRC Press, UK.
28. Anderson, R.J. and F.A.P. Petitcolas, 1996. Information hiding an annotated bibliography. http://www.petitcolas.net/steganography/bibliography/Annotated_Bibliography.pdf
29. Artz, D., 2001. Digital steganography: Hiding data within data. IEEE Internet Comput., 5: 75-80.
30. Dang, P.P. and P.M. Chau, 2000. Image encryption for secure internet multimedia applications. IEEE Trans. Consumer Elect., 46: 395-403.
31. Clarke, P.J., R.J. Collins, V. Dunjko, E. Andersson, J. Jeffers and G.S. Buller, 2012. Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light. Nat. Commun., Vol. 3. 10.1038/ncomms2172
32. Abd El-Latif, A.A., L. Li, N. Wang, Q. Han and X. Niu, 2013. A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces. Signal Process., 93: 2986-3000.
33. Hua, T., J. Chen, D. Pei, W. Zhang and N. Zhou, 2015. Quantum image encryption algorithm based on image correlation decomposition. Int. J. Theoret. Phys., 54: 526-537.
34. Zaghloul, A., T. Zhang, M. Amin and A.A. Abd El-Latif, 2014. Color encryption scheme based on adapted quantum logistic map. Proceedings of the 6th International Conference on Digital Image Processing, April 5-6, 2014, Athens, Greece.
35. Zuo, J. and D. Cui, 2009. Retrieval oriented robust image hashing. Proceedings of the International Conference on Industrial Mechatronics and Automation, May 15-16, 2009, IEEE., New York, USA., pp: 379-381.
36. Cheddad, A., J. Condell, K. Curran and P. McKevitt, 2008. Securing information content using new encryption method and Steganography. Proceedings of the 3rd International Conference on Digital Information Management, London, November 13-16, 2008, IEEE., New York, USA., pp: 563-568.

37. Ahmed, F., M.Y. Siyal and V.U. Abbas, 2010. A secure and robust hash-based scheme for image authentication. Signal Process., 90: 1456-1470.
38. Deng, S., Y. Zhan, D. Xiao and Y. Li, 2011. Analysis and improvement of a hash-based image encryption algorithm. Commun. Nonl. Sci. Numer. Simul., 16: 3269-3278.
39. Liu, Y., J. Zhang and W. Tang, 2011. Noise removal using cohen-grossberg neural network for improving the quality of the decrypted image in color encryption. Proceedings of the 3rd International Conference on Communication Software and Networks, May 27-29, 2011, IEEE., New York, USA., pp: 25-29.
40. Wu, X., 2012. A color image encryption algorithm using the fractional-order hyperchaotic systems. Proceedings of the 5th International Workshop on Chaos-Fractals Theories and Applications, October 18-21, 2012, IEEE., New York, USA., pp: 196-201.
41. Kester, Q.A., L. Nana, A.C. Pascu and S. Gire, 2013. A new encryption cipher for securing digital images of video surveillance devices using diffie-hellman-MD5 algorithm and RGB pixel shuffling. Proceedings of the European Modelling Symposium, November 20-22, 2013, Manchester, UK., pp: 305-311.
42. Ahmad, M. and O. Farooq, 2010. A multi-level blocks scrambling based chaotic image cipher. Proceedings of the 3rd International Conference on Contemporary Computing, August 9-11, 2010, Noida, India, pp: 171-182.
43. Chang, H.T. and H.E. Hwang, 2010. Multiple-Image Multiplexing Encryption Based on Modified Gerchberg-Saxton Algorithm and Phase Modulation in Fractional Fourier Transform Domain. In: Computational Collective Intelligence. Technologies and Applications, Pan, J.S., S.M. Chen and N.T. Nguyen (Eds.)., Volume 6421, Springer-Verlag, Berlin, Heidelberg, ISBN: 978-3-642-16693-8, pp: 74-80.
44. Liu, X. and Z. Li, 2011. The Application of the Pseudo Vector Multiplication in the Image Encryption Algorithm. In: Applied Informatics and Communication, Zeng, D. (Ed.)., Volume 224, Springer-Verlag, Berlin, Heidelberg, ISBN: 978-3-642-23214-5, pp: 270-277.
45. Jin, J., 2012. An image encryption based on elementary cellular automata. Optics Lasers Eng., 50: 1836-1843.
46. Zhou, Y., L. Bao and C.L.P. Chen, 2013. Image encryption using a new parametric switching chaotic system. Signal Process., 93: 3039-3052.
47. Liu, S. and J.T. Sheridan, 2013. Optical encryption by combining image scrambling techniques in fractional Fourier domains. Optics Commun., 287: 73-80.
48. Fu, C., W.H. Meng, Y.F. Zhan, Z.L. Zhu, F.C.M. Lau, C.K. Tse and H.F. Ma, 2013. An efficient and secure medical image protection scheme based on chaotic maps. Comput. Biol. Med., 43: 1000-1010.
49. Deng, X., C. Liao, C. Zhu and Z. Chen, 2013. A novel image encryption algorithm based on hyperchaotic system and shuffling scheme. Proceedings of the IEEE 10th International Conference on High Performance Computing and Communications and 2013 IEEE International Conference on Embedded and Ubiquitous Computing, November 13-15, 2013, Zhangjiajie, China, pp: 109-116.
50. Mukherji, A., 2010. Advances in smart cards application in telemedicine and biometrics. Proceedings of the International Conference and Workshop on Emerging Trends in Technology, February 26-27, 2010, Mumbai, India, pp: 770-774.
51. Sathishkumar, G.A., K. Bhoopathybagan, N. Sriraam, S.P. Venkatachalam and R. Vignesh, 2011. A novel image encryption algorithm using two chaotic maps for medical application. Commun. Comput. Inform. Sci., 133: 290-299.
52. Dong, C., H. Zhang, J. Li and Y.W. Chen, 2011. Robust zero-watermarking for medical image based on DCT. Proceedings of the 2011 6th International Conference on Computer Sciences and Convergence Information Technology, November 29-December 1, 2011, Jeju Island, Korea, pp: 900-904.
53. Bouslimi, D., G. Coatrieux, M. Cozic and C. Roux, 2012. A joint encryption/watermarking system for verifying the reliability of medical images. IEEE Trans. Inform. Technol. Biomed., 16: 891-899.
54. Sudha, G. and R. Ganesan, 2013. Secure transmission medical data for pervasive healthcare system using android. Proceedings of the International Conference on Communications and Signal Processing, April 3-5, 2013, India, pp: 433-436.
55. Huang, L., C. Wu, L. Chen and L. Zhu, 2013. Comparisons of encryption algorithms in histogram-equalized image. Proceedings of the 2013 4th International Conference on Networking and Distributed Computing, December 21-24, 2013, Hong Kong, China, pp: 80-81.
56. Wang, X.Y., Y.Q. Zhang and X.M. Bao, 2015. A novel chaotic image encryption scheme using DNA sequence operations. Opt. Lasers Eng., 73: 53-61.
57. Zhang, Y., 2015. Cryptanalysis of a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik Int. J. Light Electron Opt., 126: 223-229.
58. Zhang, S. and T.G. Gao, 2015. Encryption based on DNA coding, codon grouping and substitution. J. Electron. Inform. Technol., 37: 150-157.
59. Liu, Y., J. Tang and T. Xie, 2014. Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map. Optics Laser Technol., 60: 111-115.
60. Liu, Z., Q. Guo, L. Xu, M.A. Ahmad and S. Liu, 2010. Double image encryption by using iterative random binary encoding in gyrator domains. Optics Express, 18: 12033-12043.

61. Shan, M., J. Chang, Z. Zhong and B. Hao, 2012. Double image encryption based on discrete multiple-parameter fractional Fourier transform and chaotic maps. Optics Commun., 285: 4227-4234.
62. Wang, Q., Q. Guo and J. Zhou, 2012. Double image encryption based on linear blend operation and random phase encoding in fractional Fourier domain. Opt. Commun., 285: 4317-4323.
63. Sui, L., H. Lu, X. Ning and Y. Wang, 2014. Asymmetric double-image encryption method by using iterative phase retrieval algorithm in fractional Fourier transform domain. Opt. Eng., Vol. 53. 10.1117/1.OE.53.2.026108
64. Shao, Z., H. Shu, J. Wu, Z. Dong, G. Coatrieux and J.L. Coatrieux, 2014. Double color image encryption using iterative phase retrieval algorithm in quaternion gyrator domain. Opt. Express, 22: 4932-4943.
65. Chen, J.X., Z.L. Zhu, C. Fu, L.B. Zhang and H. Yu, 2015. Analysis and improvement of a double-image encryption scheme using pixel scrambling technique in gyrator domains. Opt. Lasers Eng., 66: 1-9.
66. Singh, H., A.K. Yadav, S. Vashisth and K. Singh, 2015. Double phase-image encryption using gyrator transforms and structured phase mask in the frequency plane. Opt. Lasers Eng., 67: 145-156.
67. Patidar, V., G. Purohit, K.K. Sud and N.K. Pareek, 2010. Image encryption through a novel permutation-substitution scheme based on chaotic standard map. Proceedings of the International Workshop on Chaos-Fractal Theory and its Applications, October 29-31, 2010, Kunming, Yunnan, pp: 164-169.
68. He, C., A. Jiang, J. Yu and B. Du, 2011. Scrambling chaotic image encryption algorithm based on contourlet. Proceedings of the 4th International Workshop on Chaos-Fractals Theories and Applications, October 19-22, 2011, Hangzhou, China, pp: 188-192.
69. Zhu, Z.L., C. Wang, H. Chai and H. Yu, 2011. A chaotic image encryption scheme based on magic cube transformation. Proceedings of the 2011 4th International Workshop on Chaos-Fractals Theories and Applications, October 19-22, 2011, Hangzhou, China, pp: 214-218.
70. Ye, R. and W. Zhou, 2011. An image encryption scheme based on 2D tent map and coupled map lattice. Int. J. Inform. Commun. Technol. Res., 1: 344-348.
71. Bhatnagar, G. and Q.M.J. Wu, 2012. Selective image encryption based on pixels of interest and singular value decomposition. Digital Signal Process., 22: 648-663.
72. Ye, R., 2013. A highly secure image encryption scheme using compound chaotic maps. J. Emerg. Trends Comput. Inform. Sci., 4: 532-544.
73. Ke, Y., Z.Q. Wang, C. Liu and K.X. Yin, 2009. Digital watermarking scheme based on chaotic encryption and DWT. Proceedings of the International Conference on Information Engineering and Computer Science, December 19-20, 2009, Wuhan China, pp: 1-4.
74. Makbol, N.M. and B.E. Khoo, 2014. A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition. Digital Signal Process., 33: 134-147.
75. Keyvanpour, M.R. and F. Merrikh-Bayat, 2011. Robust dynamic block-based image watermarking in DWT domain. Procedia Comput. Sci., 3: 238-242.
76. Elshazly, A.R., M.M. Fouad and M.E. Nasr, 2012. Secure and robust high quality DWT domain audio watermarking algorithm with binary image. Proceedings of the 2012 7th International Conference on Computer Engineering and Systems, November 27-29, 2012, Vienna, Austria, pp: 207-212.
77. Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2015. Pixel scattering matrix formalism for image encryption-a key scheduled substitution and diffusion approach. AEU-Int. J. Electron. Commun., 69: 562-572.
78. Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2015. Triple chaotic image scrambling on RGB-a random image encryption approach. Secur. Commun. Networks, 8: 3335-3345.
79. Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2015. Medical data sheet in safe havens-a tri-layer cryptic solution. Comput. Biol. Med., 62: 264-276.
80. Van Nee, R. and R. Prasad, 2000. OFDM for Wireless Multimedia Communications. 1st Edn., Artech House Inc., Norwood, MA, USA., ISBN: 0890065306, pp: 280.
81. Terry, J. and J. Heiskala, 2002. OFDM Wireless LANs: A Theoretical and Practical Guide. 2nd Edn., Sams Publishing, USA., ISBN: 13-9780672321573, Pages: 315..
82. Wang, H.D., L.Q. Huang and F. Yao, 2014. Chaotic-sequence-based channel estimation algorithm for secure optical OFDM systems. Applied Mech. Mater., 602-605: 3165-3168.
83. Quyen, N.X., L. van Cong, N.H. Long and V. van Yem, 2014. An OFDM-based chaotic DSSS communication system with M-PSK modulation. Proceedings of the IEEE 5th International Conference on Communications and Electronics (ICCE), July 30-August 1, 2014, Danang, pp: 106-111.
84. Xiao, H., K. Huo and W. Jiang, 2013. A new chaotic phase-coded OFDM signal and its characteristic. Proceedings of the Cross Strait Quad-Regional Radio Science and Wireless Technology Conference, July 21-25, 2013, Chengdu, China, pp: 349-352.
85. Sun, S., B. Rong and Y. Ju, 2013. Covert OFDM transmission using CDD based frequency selective channel. Proceeding of the IEEE Global Communications Conference, December 9-13, 2013, Atlanta, Georgia, USA., pp: 701-705.
86. Al-Dweik, A., M. Mirahmadi, A. Shami, B. Sharif and R. Hamila, 2013. Joint secured and robust technique for OFDM systems. Proceedings of the IEEE 20th International Conference on Electronics, Circuits and Systems, December 8-11, 2013, Abu Dhabi, pp: 865-868.
87. Akansu, A.N., P. Duhamel, X.M. Lin and M. de Courville, 1998. Orthogonal transmultiplexers in communication: A review. IEEE Trans. Signal. Process., 46: 979-995.

88. Hou, W., X. Wang and A. Refaey, 2013. Secure OFDM transmission based on multiple relay selection and cooperation. Proceeding of the IEEE Global Communications Conference, December 9-13, 2013, Atlanta, Georgia, USA., pp: 712-716.
89. Renna, F., N. Laurenti and H.V. Poor, 2012. Physical-layer secrecy for OFDM transmissions over fading channels. IEEE Trans. Inform. Forens. Secur., 7: 1354-1367.
90. Marvel, L.M., C.G. Boncelet and C.T. Retter, 1999. Spread spectrum image steganography. IEEE Trans. Image Process., 8: 1075-1083.
91. Cox, I.J., J. Kilian, F.T. Leighton and T. Shamoon, 1997. Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process., 6: 1673-1687.
92. Satish, K., T. Jayakar, C. Tobin, K. Madhavi and K. Murali, 2004. Chaos based spread spectrum image steganography. IEEE Trans. Consumer Electron., 50: 587-590.
93. Chandramouli, R. and K.P. Subbalakshmi, 2003. Active steganalysis of spread spectrum image steganography. Proceedings of the International Symposium on Circuits and Systems, May 25-28, 2003, Bangkok, Thailand, pp: 830-833.
94. Nugraha, R.M., 2011. Implementation of direct sequence spread spectrum steganography on audio data. Proceedings of the International Conference on Electrical Engineering and Informatics, July 17-19, 2011, Bandung, Indonesia, pp: 1-6.
95. Smith, J.R. and B.O. Comiskey, 1996. Modulation and information hiding in images. Proceedings of the 1st International Workshop on Information Hiding, May 30-June 1, 1996, Cambridge, UK., pp: 207-226.
96. Youail, R.S., V.W. Samawi and A.K.A.R. Kadhim, 2008. Combining a spread spectrum technique with error-correction code to design an immune stegosystem. Proceedings of the 2nd International Conference on Anti-Counterfeiting, Security and Identification, August 20-23, 2008, Guiyang, China, pp: 245-248.
97. Kumaravel, R. and K. Narayanaswamy, 2015. Performance enhancement of MC-CDMA system through novel sensitive bit algorithm aided turbo multi user detection. PLoS ONE, Vol. 10. 10.1371/journal.pone.0115710
98. Mushtaq, M.Z., M. Ahsan, M.S. Jamil, M. Inam ur Rehman, M. Naveed and M.S. Mushtaq, 2011. Improving quality of security for CDMA using Orthogonal coding method. Proceedings of the International Conference on Computer Science and Network Technology, December 24-26, 2011, Harbin, China, pp: 2649-2653.
99. Kondo, S. and L.B. Milstein, 1995. On the performance of multicarrier DS CDMA systems. IEEE Trans. Commun., 43: 3101-3101.
100. O'Hara, B. and A. Petrick, 2005. IEEE 802.11 Handbook: A designer's Companion. 2nd Edn., IEEE Standards Association, USA., ISBN: 9780738144498, Pages: 364.
101. Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012. Phase for face saving-a multicarrier stego. Procedia Eng., 30: 790-797.
102. Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014. Cryptic cover for covered writing: A pre-layered stego. Inform. Technol. J., 13: 2524-2533.
103. Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014. Double layer encoded encrypted data on multicarrier channel. J. Applied Sci., 14: 1689-1700.
104. Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014. Spread and hide-a stego transceiver. Inform. Technol. J., 13: 2061-2064.
105. Russell, M. and G.L. Stuber, 1995. Interchannel interference analysis of OFDM in a mobile environment. Proceedings of the IEEE 45th Vehicular Technology Conference, July 25-28, 1995, Chicago, IL., pp: 820-824.
106. Diaconu, A.V. and K. Loukhaoukha, 2013. An improved secure image encryption algorithm based on Rubik's cube principle and digital chaotic cipher. Math. Prob. Eng. 10.1155/2013/848392.
107. Riad, A.M., A.H. Hussein and A. El-Azm, 2012. A new selective image encryption approach using hybrid chaos and block cipher. Proceedings of the 8th International Conference on Informatics and Systems, May 14-16, 2012, Cairo, Egypt, pp: 36-39.
108. Feng, Y. and X. Yu, 2009. A novel symmetric image encryption approach based on an invertible two-dimensional map. Proceedings of the 35th Annual Conference of IEEE on Industrial Electronics, November 3-5, 2009, Porto, Portugal, pp: 1973-1978.
109. Wang, J. and G.P. Jiang, 2013. Image scrambling and mixing encryption algorithm based on hyper-chaotic system. Proceedings of the 32nd Chinese Control Conference, July 26-28, 2013, Xi'an, China, pp: 459-464.
110. Belazi, A., A.A. Abd El-Latif, A.V. Diaconu, R. Rhouma and S. Belghith, 2017. Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. Optics Lasers Eng., 88: 37-50.
111. Naik, K. and A.K. Pal, 2013. An image cryptosystem based on diffusion of significant bit-planes of a scrambled image with generated binary key matrices. Proceedings of the International Conference on Computational Intelligence and Computing Research, December 26-28, 2013, Enathi, pp: 1-4.
112. Sankaran, K.S. and B.V.S. Krishna, 2011. A new chaotic algorithm for image encryption and decryption of digital color images. Int. J. Inform. Educ. Technol., 1: 137-141.
113. Zhou, X., J. Ma, W. Du and Y. Zhao, 2011. Ergodic matrix and hybrid-key based image cryptosystem. Int. J. Image Graphics Signal Process., 3: 1-9.
114. Paul, A.J., P. Mythili and K.P. Jacob, 2011. Matrix based Cryptographic procedure for efficient image encryption. Proceedings of the IEEE Recent Advances in Intelligent Computational Systems, September 22-24, 2011, India, pp: 173-177.
115. Paul, A.J., P. Mythili and P. Jacob, 2011. Matrix based key generation to enhance key avalanche in advanced encryption standard. Int. J. Comput. Applic., 2: 31-34.

116. Younes, M.A.B. and A. Jantan, 2008. Image encryption using block-based transformation algorithm. IAENG Int. J. Comput. Sci., 35: 407-415.
117. Alam, M.I. and M.R. Khan, 2013. Performance and efficiency analysis of different block cipher algorithms of symmetric key cryptography. Int. J. Adv. Res. Comput. Sci. Software Eng., 3: 713-720.
118. Zhang, S., T. Gao and L. Gao, 2014. A novel encryption frame for medical image with watermark based on hyperchaotic system. Math. Problems Eng. 10.1155/2014/240749
119. Panduranga, H.T., S.N. Kumar and Kiran, 2014. Image encryption based on permutation-substitution using chaotic map and Latin square image cipher. Eur. Phys. J. Spec. Top., 223: 1663-1677.
120. Varsaki, E.E., V. Fotopoulos and A.N. Skodras, 2014. A discrete Gould transform data hiding scheme. Math. Methods Applied Sci., 37: 283-288.
121. Le, H.M. and M. Aburdene, 2006. The discrete gould transform and its applications. Proc. SPIE., Vol. 6064. 10.1117/12.643278
122. Huang, X., G. Ye and K.W. Wong, 2013. Chaotic image encryption algorithm based on circulant operation. Abstr. Applied Anal. 10.1155/2013/384067
123. Zhang, L., X. Tian and S. Xia, 2011. A scrambling algorithm of image encryption based on Rubik's cube rotation and logistic sequence. Proceedings of the International Conference on Multimedia and Signal Processing, Volume 1, May 14-15, 2011, Guilin, China, pp: 312-315.
124. Diaconu, A.V., 2016. Circular inter-intra pixels bit-level permutation and chaos-based image encryption. Inform. Sci., 355-356: 314-327.
125. Ravichandran, D., P. Praveenkumar, J.B.B. Rayappan and R. Amirtharajan, 2016. Chaos based crossover and mutation for securing DICOM image. Comput. Biol. Med., 72: 170-184.