Journal of Engineering and Applied Sciences 14 (8): 2648-2654, 2019
ISSN: 1816-949X

A Chaotic Image Encryption Method Using a Novel Compression Method for Data Embedding

Abdulrahman Alturki
Department of Electrical Engineering, College of Engineering, Qassim University, Buraydah, Saudi Arabia

Abstract: A novel technique to increase the embedding capacity of a double layered protected encryption algorithm was proposed in this study. Before, wrapping the watermarking data in the cover image DCT transformation was applied to the coefficients of the cover image. The watermarking data was compressed before embedding to reserve more space for embedding more data. This model also offers the flexibility of embedding more than one watermarks. The encryption was performed with the Arnold transformation and the Chaotic encryption algorithm to establish robust, significant and improvised data security.

Key words: Increased payload, Arnold transform, Chaotic encryption, DCT, Chaotic, embedding

INTRODUCTION

The science and communication had been advanced in such a way that the era we are living is stated as the modern era of telecommunication. The advancements made in all the domains of science had affected our lives such that human life is entirely dependent on the scientific gadgets for all the actions. In the field of communication with the development of internet in the past few decades, the entire world has been shrinked into a global village. Communication and transaction of messages are entirely made over the internet. These amelioration had risked the data security of the information exchanged over the network. There are many types of risks which includes the unauthorised duplication of data, unauthenticated access, eavesdropping, data theft, interruptions and aggressions (Pawar and Anuradha, 2015; Pawar and Agarwal, 2017; Seyyedtaj and Jamali, 2014) over the transaction, etc. According to, the survey billions of employers are fired because of data theft and a huge loss occurs to the major concerns due to data leakage many bills and laws were passed against the piracy of information. The hacking of data may end up in the fatal disasters. The above statement can be well explained with an example. The channels over which the data transactions are taking are not capable enough to protect the data and the information sent over it (Parah *et al*., 2017). The medical images are sent over the internet to the intended person who is responsible to analyse it proceed further. But if the data was hacked and modified by an unauthorised antagonist the decision taken over the modified medical data may be fatal to the corresponding patients. Thus, the protection of data is being emphasized. The available cryptographic techniques are not much effective due to the following reasons. Digital images are very high in resolution and conquers hefty storage space. Due to the large number of redundant data in such images the correlation between the adjoin pixels are very strong. In such cases the application of cryptographic techniques like DES, RSA, AES, Triple AES are not strong enough to secure the data (Wang and Wang, 2014). The cryptographic techniques makes some modifications to disguise the data, these modifications can be suspicious enough to sense the presence of confidential data in the message and paves the way for aggressions (Muhammad *et al*., 2016; Lima *et al*., 2015). Hence, there came an alternative methods to secure data by hiding the data or authenticity in the form of steganography and watermarking (Razzaq *et al*., 2017; Sharma *et al*., 2017).

Watermarking techniques are very efficient techniques to authenticate and authorise the users or possessors of the data. They not only protects the authenticity and retains the possession of the data but also used to hide the data in the multimedia objects. The security and authenticity are effective in the watermarking techniques. Various parameters like durability, visibility, significance and the capacity of the data to be hided add value to the watermarking techniques (Thanh *et al*., 2018; Rahim *et al*., 2018). Durability of an technique is ensured only if the data transmitted through this technique are able to withstand the interruptions and attacks done over it i.e., the exact data is regained even after the attacks without any deformation or disfiguring. The watermark is refereed as imperceptible if the significance or presence of

the secret data is not suspected by the intruder. The embedding capacity refers to the total number of confidential data bits that is enclosed within the watermark. For an efficient watermarking the embedding capacity should always be higher. But yet often there is a compromise between these parameters (Lei *et al*., 2017). Based on the embedding domain further, they are divided as spatial domain and frequency domain techniques. In spatial domain the transformations are directly manipulated over the pixels whereas in the frequency domains the manipulations are done over the coefficients of frequency components. Spatial technique are preferred over the frequency techniques as the implementation cost is cheap and reserves more space for embedding more data. But yet the durability offered by the spatial technique are very poor when compared to that of the frequency techniques. As the manipulations are done directly over the pixels the recovery of the disfigured pixels are not possible at the point of extraction. But whereas in the frequency techniques only the coefficients are modified and hence, they can be retrieved during extraction upon receiving the data (Panchal and Srivastava, 2015; Patel and Bhatt, 2015). The drawbacks of the frequency domain techniques is that it requies more complex manipulations and expensive. But to the effective durability and security offered frequency domain technique is used in the proposed model. Frequency domain techniques are further classified as schemes based on DCT, DWT, ILWT and SVD (Pathak *et al*., 2016; Giri *et al*., 2015).

Among the frequency domain techniques DCT is considered to be effective technique and cheaper when compared with others. In DCT the transformation can be applied either to the entire image or to the segmented blocks of the image. The transformations are applied to the coefficients and the watermarking is embedded in to the modified coefficients. The frequency components are selected as per the requirements of the applications. The selection of components are categorised as low frequency components, mid frequency components and high frequency components, respectively. To retain the ownership or copyrights of the information the watermark should be strong against the real time attacks. Hence, the watermark is embedded inside the low frequency components of the image. The low frequency components have the perceptual details of the image and hence, the modification in these components due to interruptions leads to the low quality perceptual images. Whereas to maintain the authenticity of a data the watermark has to be embedded in the high frequency components. The high frequency components are considered to be very sensitive even to the mild modifications and results in a significant distortions. Hence, these are selected for the authenticity maintenance. The stability and the insignificance of the secret data is maintained by hiding the data at the mid frequency components. The traditional encryption methods failed to prove their robustness against the attacks. With the demand of high secured encryption techniques chaos method was adopted.

The data security issues arises due to the utilization of the poor encryption techniques. The computational complexity of the techniques arises when a tough and complex manipulations are done over the coefficients. Some techniques utilizes more space for the transformation manipulations and reserves only a small portion for embedding the confidential data. Modification in the low frequency band and modification in the high frequency bands results in the apparent perceptibility and instable against attacks, respectively (Kannan and Gobi, 2015).

To overcome the common issues faced in the data security a new model of encryption technique is proposed with an enhanced reserved space for high payload. Depending upon the requirements the proposed technique is flexible for embedding multiple watermarks. In order to increase the tenacity and reserve more space for the payload the correlation between the adjoin pixels are being used. The adjoin pixels of the adjacent blocks are selected and transformed using the DCT techniques and to further increase the surveillance the Chaos encryption method is adopted in this method.

Literature review: In this digital era the digital media forms basis for all the communication and the transaction of information and data. To protect the worthwhile and important information many different techniques and methods are available. Among those area based wrapping technique is an important technique used for data security. To enhance the security double encryption scheme using the gyratory transformation and spatial domain technique was proposed by Liu *et al*. (2013). This scheme evidenced better performance than the scheme proposed by Unnikrishan *et al*. which was based on the phase encoding scheme.

The algorithms based on the linear functions are not effective as the advanced techniques. Hence, the encryption algorithm with power functions were discovered. Multi tyre protection for the information was given through the S matrix in Chaotic maps. Three different Chaotic maps were used for the protection of data. Initially, the image is segmented into matrices of order 8, then using the two dimensional cap technique the matrices were intermixed. Then with the aid of the Chaotic sequence the intermixed arrays are encrypted. The

composite technique of the Chaotic encryption and the DES method were implemented to enhance the multi level protection. The chaos sequence are also applied to reduce the iteration time complexity if the DES technique.

Zhou *et al*. (2010) proposed the DNA sequence aided encryption algorithm for the big data applications. In this algorithm the DNA sequence is utilized for the shuffling of the images by direct manipulation over the pixels and the sequence itself serves as the key to reduce the time complexity of the encryption algorithm.

For the expansion of the encryption techniques the Genetic algorithm based encryption was proposed by Enayatifar and Abdullah (2011). Then a hybrid technique of mixing the Genetic algorithm with Chaotic function was discovered.

During the extraction and reconstruction of the watermarking Compressive Sensing (CS) method is used for the effective reconstruction. This method is one of the extensively used technique and is effectively used to uphold the protection of the digital information. Then came the composite technique of CS and Arnold scrambling proposed by Sreedhanya and Soman (2012). In this technique the image is segmented into blocks and each of the blocks were transformed into 1D vectors. Then the compression and encryption were done over these vectors. The encryption of the coloured images are also possible with the chaotic maps. Safi and Maghari (2017) suggested the utilization of the double chaotic maps in the encryption of the colour images. This technique has two different phases. Each phase has separate sequence keys and produces unique key by applying XOR function over the sequence keys and the actual image. A novel encryption algorithm was discovered by diffusing the values of the pixels and confusing the pixel value position. Hyper chaotic systems were adopted for this technique. These systems are complex in behaviour and manipulations.

Thus, the Chaotic encryption along with the Arnold transformation has gained its importance in the domain of the data security. In this proposed model quantum Chaotic technique was adopted to fix the manipulated related issues and to reduce the computational complexity and manipulation time. Also, a new compression technique has been incorporated to reduce the wrapping data size, so as to increase the payload of the embedding system.

MATERIALS AND METHODS

Problem identification: In the existing technique the encryption is based on the Chaotic method and the decryption is an blind extraction. Blind decryption refers to the recovery of the original image without the details of the actual image and the embedding technique. Discrete Cosine transformations are made on the coefficients of the frequency components of the image. Here, the host image is segmented into the non imposing matrices of the order of 8. Then, DCT was applied over the matrices and the watermark is hidden inside the components by taking the difference between the DCT coefficients and the adjoin matrix. Arnold Transform along with the Chaotic encryption technique is applied over the transformed matrices.

Though two layer of encryption is provides the space reserved for the embedding of watermark is much less which leads to the poor performance of the existing techniques. The efficient hiding technique is one which offers strong security to maintain the robustness against the attacks and interruptions and should offer high payload. The term payload here refers to the number of data bits that is embedded within the host image. Hence, with this lapse a new technique is proposed to reserve more space for the embedding data.

Proposed system: The work done in the proposed is briefly explained through the flowchart block diagram as shown in Fig. 1. The proposed model is divided into two sections embedding section and extraction section. The embedding section has two phases encryption and compression. The encryption section focuses on the strong data security by providing double layer encryption to the hided data, so that, the hidden data is durable against the real time attacks and aggressions. Also, the encryption method is so, robust such that even upon the destruction of the watermark it is impossible to retrieve the hidden data without decryption algorithm and the proper key. The following sections deals with the different manipulations done in the image for encryption and compression.

Proposed encryption technique: For an effective encryption of the secret data an encryption technique based on the Arnold algorithm and Chaotic method was adopted in the proposed model. The Chaotic system is preferred for its distinct estimations, statistical unpredictability, immutability and its changing responses. These systems shows more affinity during the initialisation of the parameters. The output sequence of the chaotic method is analogous to the white noise with changing response, revised interrelation and intricacy.

The manipulations done for the intricacy of the encryption technique is given through Eq. 1:

$$Ii+1=\mu\times Ii\times(1-Ii) \quad (1)$$

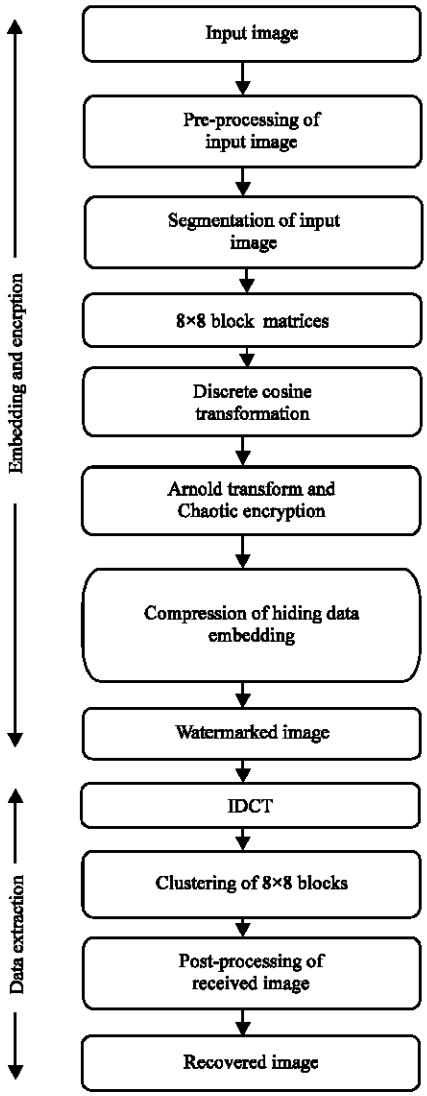

Fig. 1: Flow chart of proposed model

where, the value of μ is set within the range of [0, 4] to attain the highest certain of unpredictability. The values of the Ii can be determined based on the range of [0, i]. The initial conditions are set to obtain the Chaotic conditions of the system. This system is proved to have the high protection of the confidential data but yet to ameliorate the protection Arnold transform is composited with the Chaotic encryption. This transformation is applied over the segmented blocks of the image as the transformation works effectively in both vertical and horizontal dimensions. The mathematical representation of the Arnold transformation (Loan *et al.*, 2018) is expressed in Eq. 2:

$$[AB]_i = [1112][AB](\mathrm{mod} I) \quad (2)$$

where, the matrix of order i represent the feed image and the other matrix refers the pixel coefficients of the encrypted image. This transformation confuses and diffuses the pixel location of the actual image and outputs the different encrypted image with same data. The use of Arnold transformations is to maintain the one to one similarity with the actual image. The distinct estimation and the statistical unpredictability of this transformations makes it impossible to extract the data from the encrypted without the knowledge of the actual sequence used. The durability of this algorithm is further, made stronger as it is depending upon the number of repetition emphasis. For the decryption of the encrypted image using Arnold transformation (Loan *et al.*, 2018) Eq. 3 is used:

$$[AB]_i = [2\text{-}1\text{-}11][AB](\mathrm{mod} I) \quad (3)$$

The decryption is an blind process such that for the decryption of the data only sequence key is needed, no prior detail about the actual feed image is needed.

Watermark embedding and compression: The pre-processing unit buffers the gray-scale images and convert the coloured images into the gray-scale images. The watermark is being embedded in the luminance portion of the image, hence, for this purpose the RGB images are transformed into the YCbCr images. The changes made in the luminance attains less suspicious when compares to that of the chrominance, thus, the watermark image is embedded in the luminance portion. The one more demerit of using the embedding technique directly in the RGB images is that each plane has to be segmented into two dimensional matrices which further increases the manipulation and complexity of the embedding algorithm during extraction. Hence, the transformation of the RGB images are done.

The segmentation of the actual images into the matrix blocks of order 8 takes place after the pre processing of the feed images. The number of segmentation of the blocks depends upon the total number of bits to be embedded. Each bit is assigned to each matrix block, respectively. To embed the data without any significance the difference between the DCT coefficients and the adjoin blocks are required. So, the DCT transformations are taken prior to embedding the data. The difference between the DCT coefficients and the adjoin blocks are denoted as D. They are modified based on the data to be embedded and their value itself.

Prior to embedding double layer protection is ensured with the encryption transformation and algorithm as mentioned in the previous section. For this purpose,

the Chaotic sequence C generated the binary sequence B. The XOR operation is performed over the Chaotic sequence and the binary sequence to generate the encryption sequence depending upon the values of D the segmented blocks are divided into zones. Now depending upon the pre embedding difference the bit to be embedded is sent to the corresponding zone.

For a given block size of 16×16 only 4 bits can be embedded which limits the number of bits to be embedded inside the cover. Hence, to increase the payload the redundant bits in the watermarking images are neglected and compressed. The compression of the watermark image reduces the number of bits to be embedded in the host and increases the payload of the cover.

Extraction of watermark: The extraction process also requires the pre-processing and segmentation of the received image is done as the encryption and embedding techniques. Inverse DCT is performed over the segmented blocks and the inverse Arnold transformation is made over the blocks of the received image. The modified DCT coefficients during encryption are alone used in the inverse process. The new D is found as the difference between the DCT coefficients and the adjoin blocks. And depending upon their values they are clustered to form the actual image. The transition bits are guarded by the guard zone, so that, the extracted data does not go wrong which improves the durability of the proposed model. Though the compression was done to the water marking image the data is not deformed or disfigured even after the reduction of the redundant data.

RESULTS AND DISCUSSION

The proposed algorithm is implemented for the input image with the resolution of 512×512. The input feed image and the histogram of the input image is shown in Fig 2 and 3, respectively.

The aim of the proposed algorithm is to reduce the data to be watermarked by compression and increase the payload with the double layered encryption technique. Also, the performance study related to the parameters like PSNR, BCC, NCC are also done.

There is always a trade-off between the key parameters like durability, significance and the wrapping capacity. But in the proposed technique these factors has no settlement between them. The proposed model has the advantage of embedding the watermark both in colour and gray-scale cover. Also, it supports the embedding of more watermarks.

Significance analysis: The significance of the proposed model is very good as the embedding of the watermark

Fig. 2: Input image

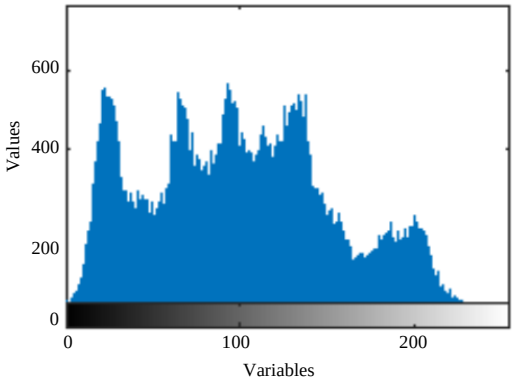

Fig. 3: Histogram of input image

data is done by manipulating the difference between the DCT coefficients and the adjoin segmented blocks values. The modification factor is normalised to the nearest available zone, so as to improvise the significance to the accepted range.

The significance of the image also defines the quality of the received image. The embedded watermark should be insignificant in such a way that the quality of the cover should not get affected and the suspiciousness of the secret data should be zero. The quality of the cover is determined by the parameters like signal to noise ration and structural similarity index. The PSNR value of the encrypted image is found to be 39.52 dB And the structural similarity is found to be 0.98. Besides, the achievement of high quality cover and fair SSI value, the proposed model e xtracts the embedded data without any error. The significance of the encrypted image and the related histogram is shown in Fig. 4 and 5, respectively.

Thus, this method offers the high quality watermarking. The quality of the watermark is maintained

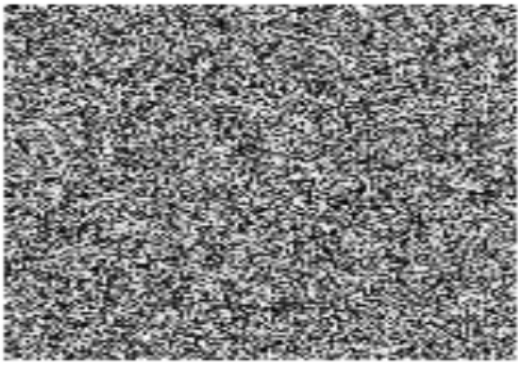

Fig. 4: Encrypted image with the watermark

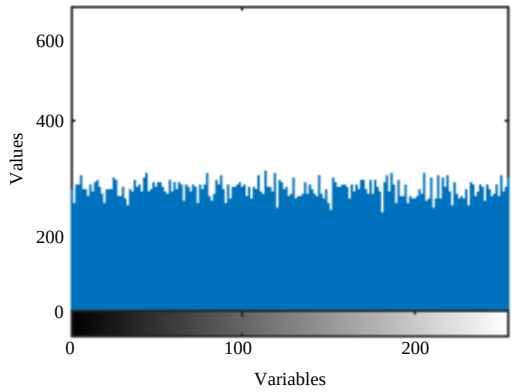

Fig. 5: Histogram of encrypted image

as the embedding of the watermark in cover causes only mild changes over the image pixels directly. Also, the embedding is done only in the lower level sub band of the cover which is responsible for the HVS parameters.

Analysis of embedding capacity: In this model all the segmented blocks are efficiently utilised to embed the watermark data bits and also, the watermark bits are compresses such that it leaves space for the other watermark data. Thus, this method shows the higher level of embedding capacity than the other existing methods. The compression is done effectively such that for the given watermarked image the number of watermark bit is 60000 and after compression it is reduced to nearly half the amount to 325000 bits. The insertion of the multiple watermarks is possible due to embedding at the luminance part of the image.

Stability analysis: The stability of the watermark is analysed by applying attacks over the encrypted image and the resulting image should be similar to that of the actual image. In the proposed model the analysis is made by applying the individual attacks and the combined attacks.

To check the stability of the cover against the geometric attacks the cover is rotated to different angles and the corresponding extracted watermarks are checked for similarity. In the proposed method the similarity index was above 0.9 and hence, it is concluded that the proposed algorithm withstand against the geometrical attacks. The obtained BER to the negligible level proves the same.

During transmission of the image the compression is done to achieve the reduced data size and faster transmission rate. During such cases the watermarked image is also compressed to lose the authenticity and ownership of the data. These led to the unrecognisable extracted image as the high frequency components are reduced as the redundant during the compression. But in the proposed system the embedding is done in the low frequency components and hence, the system is robust against the compression attacks.

Security analysis: The security of the proposed algorithm is well maintained by the combined action of the Arnold transformation and the Chaotic encryption technique. In the proposed method the decryption of the data is possible only by knowing the correct data sequence used during the encryption of the data. The data sequence here is referred to as the key. The extraction technique is considered to be blind recovery technique, so, the prior knowledge of the actual cover is not required but still the decryption process is effective with exact recovered and actual image similarity. The key used for encryption cannot be tapped by the intruder as the key sequence changes by time to time and the key is calculated by the XOR operation over the data sequence and the actual image pixel coefficients. Thus, the data security is ensured in the proposed model.

CONCLUSION

The proposed model is an blended technique of the DCT transformed image pixels encrypted by the composite Arnold transformation with the Chaotic encryption algorithm. Thus, it ensures the protection by the double layered encryption which is based on the divergence of the DCT coefficients and the values of the adjoin blocks in the segmented image. The performance analysis of the proposed model with the key parameters are analysed and the results were recorded. The resulting conclusion of the algorithm is that it is robust technique providing double layered protection with insignificance of

the embedded data. This technique has the most important advantage of increased embedding capacity by the compression of the watermarking data. The future scope of this technique involves the implementation of same with the different multimedia data for the embedding of data with the increased payload.

REFERENCES

Enayatifar, R. and A.H. Abdullah, 2011. Image security via. Genetic algorithm. Proceedings of the 2011 International Conference on Computer and Software Modeling IPCSIT Vol. 14, May 26, 2011, IACSIT Press, Singapore, pp: 198-203.

Giri, K.J., M.A. Peer and P. Nagabhushan, 2015. A robust color image watermarking scheme using discrete wavelet transformation. I.J. Image Graph. Sign. Proc., 1: 47-52.

Kannan, D. and M. Gobi, 2015. An extensive research on robust digital image watermarking techniques: A review. Intl. J. Signal Imaging Syst. Eng., 8: 89-104.

Lei, B., X. Zhao, H. Lei, D. Ni and S. Chen *et al*., 2017. Multipurpose watermarking scheme via. intelligent method and Chaotic map. Mult. Tools Appl., 1: 1-23.

Lima, J.B., F. Madeiro and F.J.R. Sales, 2015. Encryption of medical images based on the cosine number transform. Signal Proc. Image Commun., 35: 1-8.

Liu, X., Y. Cao, P. Lu, X. Lu and Y. Li, 2013. Optical image encryption technique based on compressed sensing and Arnold transformation. Opt., 124: 6590-6593.

Loan, N.A., N.N. Hurrah, S.A. Parah, J.W. Lee and J.A. Sheikh *et al*., 2018. Secure and robust digital image watermarking using coefficient differencing and Chaotic encryption. IEEE. Access, 6:19876-19897.

Muhammad, K., M. Sajjad, I. Mehmood, S. Rho and S.W. Baik, 2016. A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image. Mult. Tools Appl., 75: 14867-14893.

Panchal, U.H. and R. Srivastava, 2015. A comprehensive survey on digital image watermarking techniques. Proceedings of the 5th International Conference on Communication Systems and Network Technologies (CSNT) 2015, April 4-6, 2015, IEEE, Vadodara, India, ISBN:978-1-4799-1798-3, pp: 591-595.

Parah, S.A., F. Ahad, J.A. Sheikh and G.M. Bhat, 2017. Hiding clinical information in medical images: A new high capacity and reversible data hiding technique. J. Biomed. Inform., 66: 214-230.

Patel, R. and P. Bhatt, 2015. A review paper on digital watermarking and its techniques. Intl. J. Comput. Appl., 110: 10-13.

Pathak, S., S. Tiwari and S. Agrawal, 2016. Digital image watermarking in wavelet domain using Chaotic sequence. Proceedings of the International Conference on Futuristic Trends in Engineering, Science, Humanities and Technology (FTESHT-16), January 23-24, 2016, Institute of Professional Studies, Gwalior, India, ISBN:978-93-85225-55-0, pp: 108-113.

Pawar, M. and J. Agarwal, 2017. A literature survey on security issues of WSN and different types of attacks in network. Indian J. Comput. Sci. Eng., 8: 80-83.

Pawar, M.V. and J. Anuradha, 2015. Network security and types of attacks in network. Proc. Comput. Sci., 48: 503-506.

Rahim, T., S. Chae and S.Y. Shin, 2018. A comparative performance analysis of schemes. Proc. Korean Instit. Commun. Inf. Sci., 2018: 227-228.

Razzaq, M.A., M.A. Baig, R.A. Shaikh and A.A. Memon, 2017. Digital image security: Fusion of encryption, steganography and watermarking. Intl. J. Adv. Comput. Sci. Appl., 8: 224-228.

Safi, H.W. and A.Y. Maghari, 2017. Image encryption using double Chaotic logistic map. Proceedings of the 2017 International Conference on Promising Electronic Technologies (ICPET), October 16-17, 2017, IEEE, Deir El-Balah, Palestine, ISBN:978-1-5386-2270-4, pp: 66-70.

Seyyedtaj, M. and M.A.J. Jamali, 2014. Different types of attacks and detection techniques in mobile Ad Hoc network. Intl. J. Comput. Appl. Technol. Res., 3: 541-546.

Sharma, V.K., D.K. Srivastava and P. Mathur, 2017. A study of steganography based data hiding techniques. Intl. J. Emerging Res. Manage. Technol., 6: 145-150.

Sreedhanya, A.V. and K.P. Soman, 2012. Secrecy of cryptography with compressed sensing. Proceedings of the 2012 International Conference on Advances in Computing and Communications (ICACC), August 9-11, 2012, IEEE, Cochin, Kerala, India, ISBN:978-1-4673-1911-9, pp: 207-210.

Thanh, T.M., K. Tanaka, L.H. Dung, N.T. Tai and H.N. Nam, 2018. Performance analysis of robust watermarking using linear and nonlinear feature matching. Mult. Tools Appl., 77: 2901-2920.

Wang, X. and Q. Wang, 2014. A novel image encryption algorithm based on dynamic S-boxes constructed by chaos. Nonlin. Dyn., 75: 567-576.

Zhou, S., Q. Zhang and X. Wei, 2010. Image encryption algorithm based on DNA sequences for the big image. Proceedings of the 2010 International Conference on Multimedia Information Networking and Security (MINES), November 4-6, 2010, IEEE, Nanjing, Jiangsu, China, ISBN:978-1-4244-8626-7, pp: 884-888.