Asian Journal of Information Technology 15 (17): 3320-3326, 2016
ISSN: 1682-3915

Color Image Steganography Using Elliptic Curve Cryptographic Technique

[1]S. Prabagar and [2]S. Vasuki
[1]Department of Computer Science and Engineering, Excel College of Technology,
Komarapalayam, Namakkal Dt, Chennai, India
[2]Department of Electronics and Communication Engineering,
Velammal College of Engineering and Technology, Madurai, India

Abstract: In this research the widespread usage of ASCII art has been considered. Color image is converted into an ASCII Art by using NMF Algorithm. This art is stored as an art image. Inside this art, additional information (such as data file and mobile no or email id for sending key) is to be hidden. Both art image and hidden information are stored as stego image using 4 bit LSB Algorithm. This STEGO image is secured using Elliptic Curve Algorithm. In order to restore the original art image from stego image, the decryption key is required. This decrypting key is sent to the email id or mobile number specified during the creation of stego image. Users can decrypt the STEGO image only using the decryption key received in the mail or mobile specified. Convert the image into ASCII art, drawing the ASCII art photos is like drawing a picture in the paint application of Windows. All these processes are very easy, no experience is needed and also it is less overloaded.

Key words: ASCII art, NMF, LSB, data hiding, steganography and elliptic curve algorithm

INTRODUCTION

ASCII generator is a powerful ASCII Art generation application. It can make ASCII Art Words, ASCII Art Photos and even ASCII Art Animations easily can be made using Convert Image into ASCII Generator can take an image and process it to an HTML, RTF, BMP or TEXT file of color-coded text characters that when combined, resemble an image. It is an ASCII Art Photo and the files are very worthy of being published to the web or in the document. Also, you can make your individual ASCII Art Signatures in Convert Image into ASCII Generator. It can be use them in e-mails, documents or even in the forums on the web will be a good idea. A new method is proposed for strengthening the security of information through a combination of signal processing, cryptography and steganography. Cryptography provides the security by concealing the contents and steganography provides security by concealing existence of information being communicated. Signal processing adds additional security by compressing and transforming the information. The proposed method, viz. Steganography Based Information Protection Method (SBIPM), consists of scanning, coding, encryption, reshaping, cover processing and embedding steps (Schmidt and Laurberg, 2008).

Scanning, coding, encryption steps make the information unintelligible so that one cannot extract plain message. Embedding make the message invisible so that one cannot detect it. Reshaping spreads the message so that embedded message can be detected from distorted steganos by authorized receivers.

Information hiding: As much of today's communication is being done over technologically advanced systems (e-mail, instant messaging services, etc.), secrecy of that communication is ever present. The hidden data/file is the message which can wish to keep secret. If data looks random and adding information into this data does not change the randomness, then achieved the steganography

Since this byte can contain any value, this implies randomness. By changing the Least Significant Bit (LSB) of any byte within the image file, a human eye viewing the image will not be able to tell a difference from one shade to the next. This allows us to only hide a message one-eighth the size of the original cover file. This is not much you think that having a cover image of 128 bytes will only yield us a 16 byte hidden message (Shashua and Hazan, 2005).

The growing field of cyber forensics detective work in the digital domain should create greater demand for steganalysis tools in the near future.

Corresponding Author: S. Prabagar Department of Computer Science and Engineering, Excel College of Technology, Komarapalayam, Namakkal Dt, Chennai, India

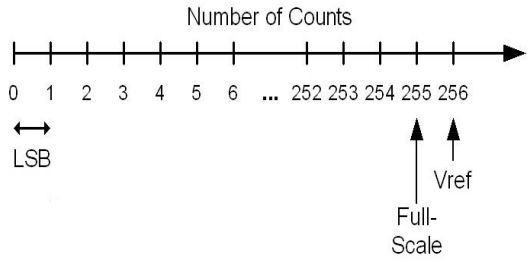

Fig. 1: Working of NMF Method

Non negative matrix factorisation: Non-negative Matrix Factorization (NMF), also non-negative matrix approximation is a group of algorithms in multivariate analysis and linear algebra where a matrix V is factorized into (usually) two matrices W and H with the property that all three matrices have no negative elements. This non-negativity makes the resulting matrices easier to inspect. Since, the problem is not exactly solvable in general, it is commonly approximated numerically shown in Fig. 1 (Shashua and Hazan, 2005). NMF finds applications in such fields as computer vision, document clustering, chemo metrics and recommended systems.

Standard NMF algorithm: Given a non-negative matrix V∈R = 0, M×T, the goal is to approximate V as a product of two non-negative matrices W £ R≥0, M×R and H £ R≥0, R×T:

$$v \approx WH, v_{ik} \approx \sum_{J=1}^{R} W_{ij} h_{jk} \quad (1)$$

Typically, R<M where, W contains a low-rank basis and H contains associated activations. Two NMF algorithms were introduced by Pooyan and Delforouzi (2007), each optimizing a different cost function to measure reconstruction quality. The cost functions specified are the Squared Euclidean Distance (SED):

$$D_{SED}(V, W, H) = 1/2||V-WH||^2 \quad (2)$$

Ascii art conversion using non-negative constraints: To increase the flexibility of our NMF algorithm β-divergence is employed as its cost function. The Beta Divergence (BD) (proposed as an cost function for NMF by (Cichocki *et al.* (2006) also referred to as the modified alpha divergence is a parameterized divergence measure that encompasses the previously discussed cost functions of SED and KLD and the Itakura-Saito Divergence (ISD).

$$D_{ISD}(V||W, H) = \sum_{Ik} (V_{ik\,log}\_V_{ik}\text{-}V_{ik}\text{+}[WH]_{ik}) \quad (3)$$

of the image is indicated by H:

$$V \approx W \text{ maxcol } (H, Q) \quad (4)$$

MATERIALS AND METHODS

Steganography: Steganography is a useful technique for hiding data behind the carrier file such as image, audio, video etc. and that data securely transfer from sender to receiver. The cryptography is also another technique which is used for protecting information. The combining encryption method of cryptography and steganography enables the user to transmit information which is masked inside the file in plain view. This will provide more security to transfer the data.

This study provides a general overview of steganography techniques in which text, image audio and video medias are used for the information hiding behind channels.

Least Significant Bit (LSB): The Least Significant Bit (LSB) is the bit position in a binary integer giving the unit value that is determining whether the number is even or odd. The LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digits further to the right. It is analogous to the least significant digit of a decimal integer which is the digit in the ones (right-most) position (Sutaone and Khandare, 2008).

It is common to assign each bit a position number, ranging from zero to N-1 where N is the number of bits in the binary representation used. Normally, this is simply the exponent for the corresponding bit weight in base-2 (such as in $2^{31}..2^{0}$).

The least significant bits have the useful property of changing rapidly if the number changes even slightly. For example, if 1 (binary 00000001) is added to 3 (binary 00000011), the result will be 4 (binary 00000100) and three of the least significant bits will change (011-100). By contrast, the three most significant bits stay unchanged (000-000).

Least significant bits are frequently employed in pseudorandom number generators, hash functions and checksums in Fig. 2 (Kompass, 2007).

Cryptography: Cryptography is the study of techniques for secure communication in the presence of third parties. More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and

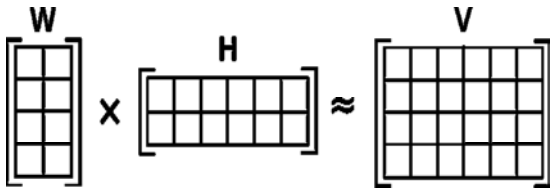

Fig. 2: LSB counts

which are related to various aspects in information security such as data confidentiality, data integrity, authentication and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science and electrical engineering. Applications of cryptography include ATM cards, computer passwords and electronic commerce.

Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same. Since, World War I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system but it is infeasible to do so by any known practical means (Fig. 3).

Steganography versus cryptography: The comparison between steganography and cryptography is illustrated in Table 1.

Elliptic Curve Cryptography (ECC): It involves encryption and decryption of messages. The core of cryptography lies in the keys involved in encryption and decryption and maintaining the secrecy of the keys. Another important factor is the key strength, i.e., the difficulty in breaking the key and retrieving the plain text. There are various cryptographic algorithms. In this paper we use Elliptic Curve Cryptography (ECC) over Galois field. This system has been proven to be stronger than known algorithms like RSA, DSA, etc., (Narayana and Prasad, 2010). Our aim is to build an efficient elliptic curve cryptosystem for secure transmission or exchange of confidential emails over a public network.

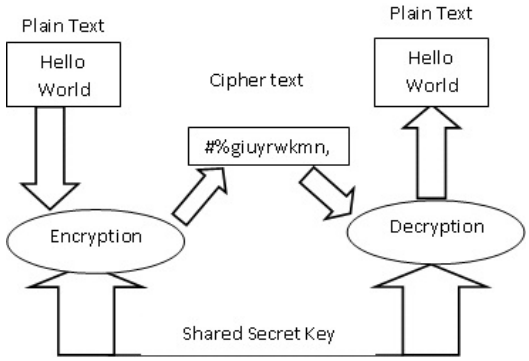

Fig. 3: Cryptography technique

Table 1: Comparison between

Context	Steganography	Cryptography
Host file	Image, audio, text, etc	Mostly textfiles
Hidden file	Image, audio,text, etc	Mostly text files
Result	Stego file	Cipher text
Type of attack	Steganalysis: Analysis of a file with a objective of finding whether it is stego file or not	Cryptanalysis

Review work on elliptic curve cryptography

Overview: The mathematical operation of ECC is defined over the elliptic curve: $y2 = x3+ax+b$ where $4a3+27b2 = 0$. Each value of 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfy the above equation plus a point at infinity lie on the elliptic curve. The major advantage of ECC over RSA is that, it requires much shorter key lengths for ensuring the same level of security. For example, 160 bit key in ECC is considered to be as secured as 1024 bit key in RSA. The fastest known technique for taking the elliptic curve logarithm is known as the Pollard rho method. Here also ECC performs better than RSA. Moreover, security of ECC grows exponentially with its parameters while that of RSA grows sub-exponentially. The comparison of key sizes of RSA and ECC for providing the same level of security. The disadvantage of ECC is that it involves much computation and hence is complex (Fig. 4 and Table 2).

Types of attacks: Attacks and analysis on hidden information may take several forms: detecting, extracting and disabling, destroying or modifying hidden information. An attack approach is dependent on what information is available to the steganalyst (the person who is attempting to detect steganography-based information streams). The possible attacks on a stego media can be one of the following:

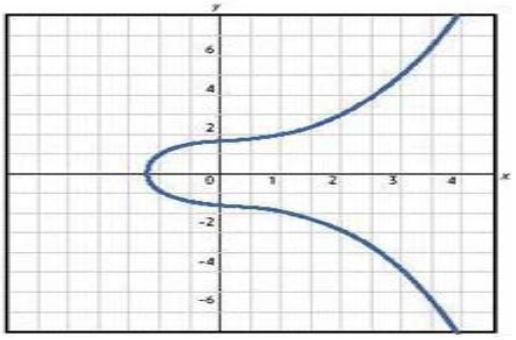

Fig. 4: An elliptic curve

Table 2: Comparison of key sizes of rsa and ECC

Rsa key size (bits)	ECC key size (bits)
1024	160
2048	224
3072	256
7680	384
15360	512

- Steganography-only attack: Only the steganography medium is available for analysis
- Known-carrier attack: The carrier that is the original cover and steganography media are both available for analysis
- Known-message attack: The hidden message is detected and available for analysis
- Chosen-steganography attack: Both the steganography medium and tool (or algorithm) are known
- Chosen-message attack: A known message and steganography tool (or algorithm) are used to create steganography media for future analysis and comparison. The goal in this attack is to determine corresponding patterns in the steganography medium that may point to the use of specific steganography tools or algorithms

Existing system: Images that are converted to text where some touch up work is done after the conversion. In previous if any text is typed on the image means it will be erased automatically. Make your pictures eye-catching with a very cool texture composed of letters and digits. ASCII Art Generator is an amazing graphics art to text art solution which allows you to convert digital pictures into full color text-based images easily and quickly. Input can any message you'd like and let your picture say what do want it to read. It supports gif, jpg, bmp files and generates four popular formats including html, image, rtf and ASCII.

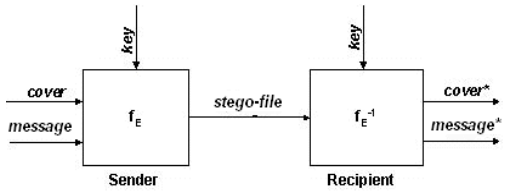

Fig. 5: Overall structure of the steganographic system

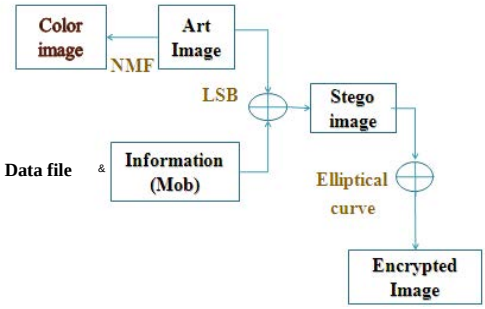

Fig. 6: Encryption process

RESULTS AND DISCUSSION

Proposed system implementation: The objectives of this work are to design and implement a steganographic system which integrates a ASCII Art module and an encryption module to improve its capacity and security requirements. The different phases involved are discussed.

Color image is converted into an ASCII Art using NMF Algorithm. This ASCII art is stored as an art image. Inside this art, additional information (such as data file, mobile no or email id) is to be hidden. Both art image and hidden information are stored as stegoimage using 32 bit LSB Algorithm. This STEGO image is secured by using Elliptic Curve Cryptography algorithm. The decrypting key is sent to the mobile hidden in the image. Users can decrypt the STEGO image only using the decryption key received in the mobile specified.

Figure 5 shows the overall structure of the steganographic system where fE denotes the steganographic embedding function and fE-1 the steganographic extracting function.

The steganographic system allows the encoding and hiding of secret messages in cover image files. The encryption and decryption algorithms implemented are the ECC algorithm using C#. NET libraries. The complete process which involves encryption and hiding information is shown in Fig. 6.

Encryption process: The method is reasonably simple and have a key matrix $K_L \times 2$ where:

$$\forall = 1, L; L \geq 16$$
$$K_{ij} \in \{1, 2, 3, 4, 5, 6, 7, 8\}$$
$$\forall = 1, 2_j$$

This key is known only to the sender and receiver. When the first party wants to send a message M to the second party, he/she determines the key 2 LK and every character from the message is replaced by a binary value. An eight-bit octet is generated randomly and set in a temporary vector V. the bits in the vector V from position K[1, 1] to position K[1, 2] are replaced by bits from the secret message.

Then the resulting vector V is stored in a file. As long as the message file has not reached its end yet, we move to the next row of the key matrix and another octet is generated randomly and the replacement is performed repeatedly and the resulting vector is stored in the file. The previous procedure is repeated over and over again pending the end the message. The resulting file is sent to the receiver who beforehand has the key matrix. If the key Length is not enough to cover the whole message during the encryption process, the key will be reapplied over and over again until the encryption of the whole message is completed.

Decryption process: For decrypting the received encrypted file the following steps are taken. An octet is read from the encrypted binary plain text message EBPM file, then it is set in a temporary vector V from this vector, bits are extracted from position K(1, 1) to position K(1, 2) and set in a BPM file. Since the EBPM file is nonetheless not empty, the next octet is read from the EBPM file and then it is set in a temporary vector V. From this vector, bits are extracted from position K(2, 1) to position K(2, 2) and added to the binary plain text message BPM file. The above steps are repeated over and over again until the EBPM file becomes empty. Every octet form the BPM file is transformed to the corresponding character and then is put in the plaintext file. When the EPBM is empty the plaintext file becomes the message (Fig. 7).

In case that the key length is not enough to cover the whole message during the decryption process, the key will be reapplied over and over again till the decryption of the whole message is completed.

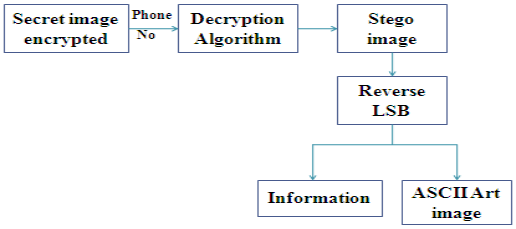

Fig. 7: Decryption process

Explanation of entire process: In our Encryption process, Normal image is converted into ASCII Art by using the Non Negative Matrix factorization algorithm. This NMF is a group of algorithms in multivariate analysis and linear algebra where a matrix V is factorized into (usually) two matrices W and H with the property that all three matrices have no negative elements.

Inside this art, additional information with mobile no is to be hidden. Both art image and hidden information with mobile number are stored as stegoimage using 32bit LSB Algorithm in this LSB algorithm have the useful property of changing rapidly if the number changes even slightly.

This STEGO image is secured using Elliptic Curve Cryptography algorithm. Our aim is to build an efficient elliptic curve cryptosystem for secure transmission or exchange of confidential emails over a public network.

In order to restore the original art image from stegoimage, the decryption key is required. This decrypting key is sent to the mobile number specified during creating stegoimage. Users can decrypt the STEGO Image only using the decryption key received in the mail specified.

Experimental results

Encryption process: Steps involved are:

- Firstly, load the image and the image automatically converted as ASCII art
- Secondly, merge the ASCII image and data file and get the stego-image
- Thirdly, use the ECC to encrypt the stego-image
- Finally, save the encrypted file (Fig. 8 and 9)

Decryption process: Steps involved are:

- Load the image file saved after the encryption
- Assign location to save the decrypted file
- Decrypt the file using NEFT key for the stego-image
- Original data file separated (Fig. 10)

Fig. 8: Image to ASCII art conversasion

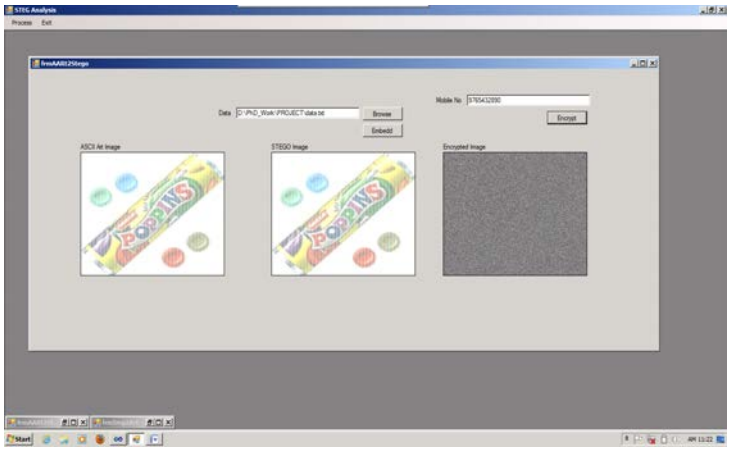

Fig. 9: Encryption of stego-image using ECC

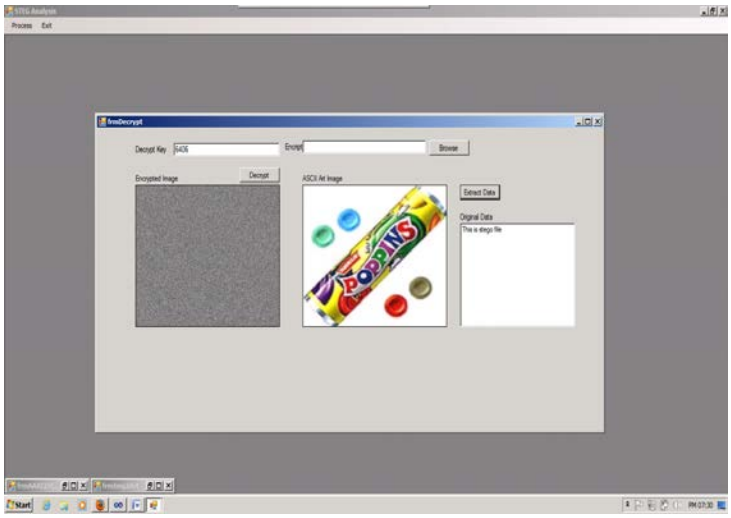

Fig. 10: Decryption of stego-image using NEFT key

CONCLUSION

In this application is presented a novel application of NMF related methods to the task of automatic ASCII art conversion where a binary image is fitted to a basis constructed from mono space font glyphs using a winner-takes-all assignment. When compared to a standard pseudo inverse approach, non-negative constraints minimize the black space of the ASCII art image, producing better defined curves. Furthermore, propose the use of the divergence cost function for this task as it provides an element of control over the final ASCII art representation.

Thus, it is concluded that the strength of security achieved is very high and unauthorized receiver will not be able to get back the original message using exhaustive without the knowledge of key parameters.

Digital steganography is interesting field and growing rapidly for information hiding in the area of information security. It has a vital role in defense as well as civil applications. In future, we will have more secured systems based on this technology. In all cases though, the system needs to fulfill the needs of today and future.

REFERENCES

Cichocki, A., R. Zdunek and S. Amari, 2006. Csiszar`s divergences for non-negative matrix factorization: Family of new algorithms. Lecture Notes Comput. Sci., 3889: 32-39.

Kompass, R., 2007. A generalized divergence measure for nonnegative matrix factorization. Neural Comput., 19: 780-791.

Narayana, S. and G. Prasad, 2010. Two new approaches for secured image steganography using cryptographic techniques and type conversions. Signal Image Process. Int. J., 1: 60-73.

Pooyan, M. and A. Delforouzi, 2007. LSB-based audio steganography method based on lifting wavelet transform. Proceedings of the IEEE International Symposium on Signal Processing and Information Technology, December 15-18, 2007, Giza, Egypt, pp: 600-603.

Schmidt, M.N. and H. Laurberg, 2008. Nonnegative matrix factorization with Gaussian process priors. Comput. Intell. Neurosci., Vol. 2008, 10.1155/2008/361705.

Shashua, A. and T. Hazan, 2005. Non-negative tensor factorization with applications to statistics and computer vision. Proceedings of the 22nd International Conference on Machine Learning, August 07-11, 2005, ACM, New York, USA, pp: 792-799.

Sutaone, M.S. and M.V. Khandare, 2008. Image based steganography using LSB insertion technique. Proceedings of the IET International Conference on Wireless, Mobile and Multimedia Networks, January 11-12, 2008, Mumbai, India, pp: 146-151.