RESEARCH ARTICLE OPEN ACCESS

A Hybrid of Steganography and Cryptography for Decreasing Mean Square Error and Bit Error Rate

Poonam Yadav, Maitreyee Dutta
ME Scholar, Department of Electronics & Communication Engineering, NITTTR, Chandigarh, India
Professor, Department of Computer Science & Engineering, NITTTR, Chandigarh, India
Corresponding Author: Poonam Yadav

***ABSTRACT*: *Internet, being the common platform for information sharing among people has increased its importance in digital world. To keep this online sharing unrevealed or to save it from being stolen, some security measures are developed such as Watermarking, Cryptography and Steganography. Watermarking is the visible marking for copyright protection; Cryptography is to encrypt the data to make it difficult to understand whereas Steganography is covert writing for obscuring the information. Various features such as invisibility, payload capacity, robustness and imperceptibility make steganographic mechanism different and useful in comparison to watermarking and cryptography. There are some legitimate as well as illegitimate applications of steganography. When keeping security in point of view in order to protect the data, steganography is often more advantageous and its illegitimate uses can be overcome by legitimate ones. This paper gives an overview of steganography domains and their suitable field of application. In this paper, steganography and cryptography are combined to form a hybrid so as to attain low MSE as well as low BER by the use of space domain. The entropy achieved is 7.69.*

***KEYWORDS*: *Steganography, Image domain, Transform domain, Security, Cryptography, MSE, BER.*

Date of Submission: 26-10-2017 Date of acceptance: 04-11-2017

I. INTRODUCTION

As information is an important source of communication thus its security is essential especially when we are working with real time systems which can be categorised into hard and soft real time systems. Hard real time systems include air traffic control and command control systems whereas soft real time systems include online transactions and flight reservation systems. These systems are at risk due to phishing, denial of service attacks, eavesdropping, virus attacks etc [1]. Hence, these systems should and must be kept secured by using various developed security techniques available such as Watermarking, cryptography and steganography. Their history can be traced back to ancient era when watermarking introduced in paper making industry to mention the paper brand in the late middle ages (13th Century) and then later currencies and post stamps were watermarked in many countries to harden the counterfeiting [2]. Digital watermarking was introduced in 1989 for illegal copies detection [3]. Its widely used applications are tamper-proofing and copyright protection. Cryptography is an ancient art and science of writing in secret code, its first documented use dates back to circa 1900 B.C. when an Egyptian scribe used non-standard picture symbols in an inscription [4]. Cryptography also got its historical name by Julius Ceaser during 100 B.C. - 44 B.C. named as Ceaser cipher [5]. Steganography derived from the Greek word 'στεγανω' which means 'covert writing'. The father of history named Herodotus described many instances related to steganography. The first instance was of Demaratus in 440 BC when a warning was being sent to Greece written on wax tablets with wooden back with re-writable surfaces. Second instance was of Histiaeus, who provoked revolt against Persians where the message of revolt was sent by his entrusted slave by tattooing message on shaved head and sent him when hairs regrew. Also, during World War II, French people transfer their messages about the war using invisible ink at the couriers back and espionage used minute sized microdots produced photographically that were detected only by the glancing light [6]. There are many more instances that describe the steganography as benchmark from ancient era till the modern era. The organisation of this paper is as follows: History of security techniques is briefly explained in this section, classification of steganography and cryptography is mentioned in section 2, proposed work discussed in section 3, simulation results in section 4 and finally section 5 concludes the paper.

II. CLASSIFICATION OF STEGANOGRAPHY

A steganographic system can be counter played by an adversary observation that a file contains hidden information in it, while counter playing on a watermarking system signifies the removal of the trademark but not to trace that mark [7]. There are various categories of steganography as shown in Fig. 1.

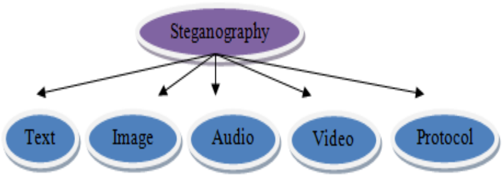


Fig. 1 Classification of Steganography

Text Steganography: Here, data is hidden inside the cover text file. Text steganography with digitization is not used very often since text files have very limited duplicate data. Historical and the most usual method of steganography is to hide data in text. The intention was to veil secrecy in every kth alphabet of 1 byte of data which is in the form of text. Because of internet and digitization these methods have lessen up its importance.

Image Steganography: Here, data is hidden in cover image. A prominent data can be hidden efficiently inside an image as it has huge amount of redundant information, as a result they are often times used cover media for steganography.

Audio Steganography: As the name suggests, the data in this type of steganography is hidden inside an audio file. It is done by optimizing the audio signal so that the changes are imperceptible to unauthorized personnel.

Video Steganography: Here, video file is used to hide the data. In video steganography, hidden data is difficult to perceive by mind or senses as changes in the pixels of video frames are impossible to detect.

Protocol Steganography: Hiding information within messages having network control protocols or network control program used in transmitting the data is termed as protocol steganography [8]. In the layers of the Open System Interconnection network model, steganography can be used as covert channels are available in the layers [9].

a) Steganographic Domains

Many categories of steganography thrived in ancient India and China, also by military mediators where they used a thin piece of silk or paper to hide secret messages and the motive was that only anticipated recipient knew about existence of information. To avoid this destruction, information security system was developed consisting of various domains in terms of steganography and cryptography as explained below. The embedment of data is directly in the intensities of pixels of an image in case of spatial domain. That is why spatial domain is sometimes referred as Image domain [10]. Spatial domain algorithms encompass on bit wise insertion and the image file formats suitable are lossless compression methods [11], usually it depends upon the type of image format for the compression to be lossy or lossless. Various spatial domain algorithms are discussed below:

- **LSB Substitution:** The simplest algorithm and most commonly used steganographic method is the one in which the message is inserted into the least significant bit. To potentiate payload capacity one or more bits can be paired to be embedded into a single pixel. Least significant bit insertions can be either of variable or fixed size. The fixed size insertion as the name implies embeds same number of bits every time in each pixel of cover media whereas, variable size indicates the bits embedding depending upon the contrast and luminance characteristics [10]. The idea behind the hiding message in LSB is that not many changes can be seen in image and it appears same as the original image. For example, 3 pixels of 18-bit image grid is given as

(101101	11100	01100)
(100110	00100	01100)
(010010	01101	00011)

The resulting grid when a number 125 whose binary representation is 01111101 is embedded into least significant bit will be

(10110**0**	1110**1**	0110**1**)
(10011**1**	0010**1**	0110**1**)
(01001**0**	0110**1**	00011)

- **PVD Based:** Despite of more payload capacity of the concealed information, Pixel Value Differencing has the ability to provide a high quality stego image, i.e., whether it is an edged area pixel or smoothed area pixel, is being decided by the amount of insertion bits. In edged area there is high difference value between the adjacent pixels, whereas in smooth area it is less it means more number of bits can be inserted in edge areas than smooth areas. While human visual percept has low sensitivity towards elusive changes in edge areas of a pixel, it is more susceptible to changes in the smooth areas. This method hides the data in the target pixel by finding the characteristics of four pixels surrounding it as shown in Fig. 2.

N(x-1,y-1) **Top Left Pixel**	**N(x-1,y)** **Top Pixel**	**N(x-1,y+1)** **Top Right Pixel**
N(x,y-1) **Left Pixel**	**N(x,y)** **Target Pixel**	

Fig. 3 PVD’s Pixel pattern arrangement

- **Histogram Based:** Histograms can also be used to embed the secret data. Histogram shifting process generates the pixel locations. Firstly, histogram of cover medium is generated, then least frequent and more frequent pixels with their occurrence number are found out and stored and then raster scan procedure is done to read the whole image for embedding the data. General Histogram based method results in less payload capacity. To increase the payload capacity Adjacent Pixel Difference (APD) is used which generates pixel difference sequence histogram. A stego image with high visual degree can be maintained with APD but with limited embedding capacity [12].
- **Color palette based:** This steganographic technique was designed and developed for palette based images such as Graphic Interchange Format (GIF) files. The total number of colors maximally this type of file can store is 28 = 256 as it has 8 bits [13]. The images with colors stored in palette are the indexed images and this color palette is sometimes referred as color look up table [14]. Also, to reduce or to save the look up time the colors are sequenced from their maximum usage to least usage.
- **Pseudo noise sequence:** In image steganography, frequencies of high range have greater relevancy for obscuring the information concealed but are not that effective as far as the robustness is concerned rather frequencies in lower range are robust but because of having unacceptable visible impact they are merely used. Spread spectrum can conciliate this inconsistency when in each frequency band a low-energy signal is allowed to be embedded [15]. When concealed data is scattered all throughout the cover media making its detection difficult, then a name called spread spectrum arises. Communication through spread spectrum can be defined as the procedure in which bandwidth of a narrowband signal is dispersed widely all over a broad band of frequencies and is attained by co-ordinating the narrowband waveform with a broadband waveform [16]. As soon as dispersion is done it can be seen that the energy of the narrowband signal in any one frequency band is low and results in harder detection. In SSIS, the data is embedded in noise and this noise along with cover image gives stego image. As the influence of the cover image is much higher than that of the embedded signal, perceptibility of embedded image to man’s eye or by computer analysis without access to the original image is difficult [16].

b) Cryptographic Domains

Cryptography is the act of writing data in codes and ciphers and making it unintelligible so that nobody can access it without given methods or keys. It also includes digital signatures, authentication and secret sub-storage [1]. Cryptology is the Greek word which means science of analysing and deciphering codes. Cryptography is the collection of cryptographic mechanisms which includes ciphering and deciphering algorithm, integrity check functions and digital signature methods. Cryptographic algorithms are categorized into symmetric and non-symmetric key algorithm. Symmetric key algorithms have the same key to cipher and decipher the message. It is further partitioned into block ciphers (fixed size blocks of symbols) and stream ciphers (continuum stream of symbols). A non-symmetric key algorithm uses pair of cryptographic keys although distinct but has mathematical relation. There are two separate keys namely as public key and private key. For encrypting purpose, a public key is used by the source whereas for decrypting the message a recipient makes use of private key. Cryptography algorithm includes: DES, AES and RSA. The most popular and commonly used among all is RSA encryption algorithm because of its high imperceptibility.

- **DES:** The abbreviation to DES is Data Encryption Standard which is a popular and widely used ciphering algorithm based on symmetric key concept. This is called a symmetric key algorithm as one private key is shared by both sender as well as the receiver which weakens its security level. DES is applied on a block of data at a time rather than single bit

[17]. It groups the data to be ciphered into a block consisting of 64-bits. As there are chances of out flowing of key as single key is used. It was used where strong encryption was required. As it was the first encryption method thus it was quickly adopted by the industries. Soon, DES was succeeded by AES because of its lack of security.

- **AES:** It stands for Advanced Encryption Standard which is also a symmetric key algorithm as like DES. It allows for three different length of the keys to be used for ciphering and they are 128, 192 or 256 [18].
- **RSA:** This is another method of ciphering the text for secure communication in cryptography. RSA is asymmetric key algorithm in which there are two different keys used by the sender as well as the receiver; they are public key and private key. This is the most commonly used cryptographic method. This method is secured as there are two different keys for encryption.

III. PROPOSED WORK

In proposed work, a cover image which is an RGB image is taken in which RLE encrypted message is embedded by the use of cryptographic mechanism which is RSA encryption along with Diffie Hellman Key exchange. Then, to spread the secret message over an entire image, pixel locations are calculated by the method of PN sequence generation. Then, secret bits are replaced by bits of these pixel locations with LSB technique. The detailed explanation of insertion algorithm and extraction algorithm is given as below:

- **Insertion Algorithm**

1) The text file which is to be hidden is read.
2) String conversion is performed which converts ASCII text to character type text.
3) After the character text is obtained it is then converted into decimal form.
4) On this converted decimal secret information RSA encryption is applied followed by Diffie Hellman Key exchange algorithm to obtain the stego keys and the algorithm is as follows:

RSA Encryption Algorithm:

a. Choose two large prime numbers namely as ‘p’ and ‘q’.
b. Calculate modulus, n= p × q.
c. Select another number named as ‘e’ relatively prime to totient $\phi(n) = (p-1) \times (q-1)$ such that $1 < e < \phi(n)$.
d. Compute an integer‘d’ from the following relation: $d= \{1+ \phi (n)\}/e$.
e. Here, ‘e’ is public key exponent whereas‘d’ is private key exponent [19].

Diffie-Hellman key exchange algorithm for key generation:

a. For public key following equation is used: $C=M^e \bmod n$, where C is cipher text and M is message to be encrypted.
b. For private key used by receiver to decrypt the message, $M=C^d \bmod n$ (n is the modulus calculated above) [60].

5) The encrypted message is then compressed by using RLE compression technique- a lossless technique and it is explained with the help of an example. Suppose, a message to be hidden is having following pattern ‘ttttttttrrrrrrrrraaaaafffffffiiiiiiiiccccccjjjjjaammmmm’, after encoding it will be 8t9r5a7f8i6c5j2a5m. Here, identical intensities are represented as run-length pairs which form a group having count of repetition first and then followed by the repeated symbols. Here, ‘895786525’ code is taken as the ‘data key’ and encrypted form of ‘traficjam’ is taken as ‘encrypted data’.
6) Compression ratio is calculated by taking the ratio of length of encrypted data to the actual length of secret information.
7) Now, the message to be hidden is encrypted and compressed.
8) Next step is the hiding procedure and for that first of all cover image is taken of any format such as bmp, png, jpg, etc. of size 512×512 pixels.
9) The data key obtained is hidden in the layer 1 i.e. pixels of Red component and encrypted data is hidden in layer 2 i.e. pixels of Green component of RGB image.
10) Now, the data as well length are converted from decimal to binary.
11) To keep the standard length, the data is made 20-bit by zero padding.
12) After that random pixel locations are calculated and these locations are also converted into binary form to make it compatible with actual data length, length of data in binary form and the key.
13) The random locations will be generated keeping in mind its uniqueness so that no two bits of secret message are hidden at same location.
14) The hiding concept follows LSB substitution scheme and last two bits of random pixel locations are replaced by the last two bits of the secret message.

    For example, let us suppose that one of the unique pixel locations found is 12. The binary conversion of this location is (000000000000000011**00**). It can be seen that zero padding is done in order to make the location 20-bit. The one of the character of encrypted message in binary form is (000000000000000111**01**). The last two bits **‘00’** of pixel location are replaced by the corresponding last two bits **‘01’** of encrypted message and next two bits **‘11’** of encrypted message from the last are replaced by last two bits of another pixel location. This is how the whole encrypted message is hidden into the randomly selected pixels.
15) Thus, a Stego image is obtained.

How information is being extracted from the image at the receiver end is described further in the extraction algorithm.

- **Extraction Algorithm**

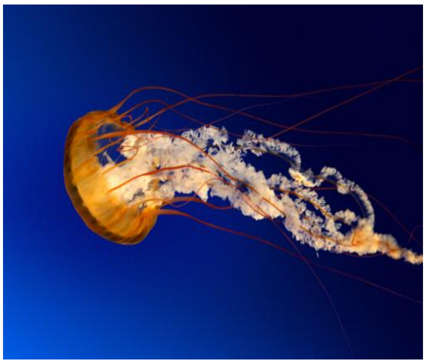
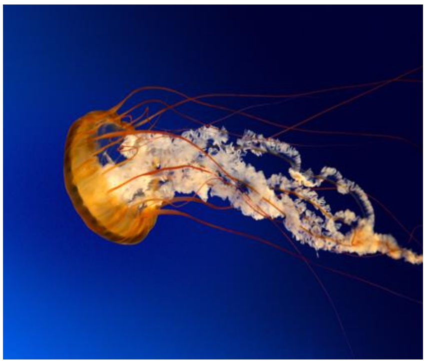
1) Stego image is read.
2) Data is key is extracted from the image.
3) Decoding of the key is done by Run length decoding method.
4) Then decoded message is decrypted by applying RSA decryption.
5) Decrypted message is again converted back to string from decimal form.
6) Finally, the secret information is obtained without any degradation in the quality of original cover image.
7) Error check is also done to ensure that message sent by the source is same as the message received at the destination end.

IV. SIMULATION RESULTS

MATLAB software is utilised for simulation of the hiding algorithm. Images of 512×512 size are taken as hiding medium. Images taken are desert; penguin and jelly fish all of .jpg format. Qualitative analysis is done on the basis of MSE, PSNR and BER.

a) Qualitative Analysis

Table 1- Cover images and Stego images

Image details (512×512)	Cover Image	Stego Image
1. JellyFish.jpg		
2. Penguin.jpg		
3. Desert.jpg		

b) Quantitative Analysis

Table 2 MSE and BER of the images

Image Detail	MSE	BER	PSNR
1. JellyFish.jpg	0.0019	0.0133	75.4142
2. Penguins.jpg	0.0019	0.0133	75.3236
3. Desert.jpg	0.0019	0.0133	75.3966

IV. CONCLUSION

The proposed work concludes that the hybrid of steganography and cryptography is quite beneficial in transmission and reception of the secret message covertly. Here, MSE achieved is 0.0019, average weighted PSNR achieved is 75dB approx and BER is of value 0.0133. Thus, low MSE and BER signifies that there is minimum error between the original image and the stego image i.e. the image obtained after hiding the text. This method has wide variety of application in various sectors of government, digital signatures, computer security and so on. More and more security techniques are in demand as the number of intruders is increasing day by day.

REFERENCES

[1]. Tsai, J. J. P.:"Attacks and countermeasures in system security", International Conference on E-commerce Technology for Dynamic E-Business, IEEE, 2005.

[2]. Shih, F.: "Digital Watermarking and Steganography: Fundamentals and Techniques", Studies in Computational Intelligence, (CRC Press, Taylor & Francis Group, 2009, Special Indian Edition, 2012), pp. 1-6.

[3]. Komatsu, N., Tominaga, H.: "A Proposal on Digital Watermark in Document Image Communication and its Application to Realizing a Signature", Transaction of Institute of Electronics, Information and Communication Engineers, 1989.

[4]. Rajni Devi, T.: "Importance of Cryptography in Network Security", International Conference on Communication Systems and Network Technologies, IEEE, 2013.

[5]. Litwin, L.: "Cryptography", IEEE Potentials, 2001, Vol. 20, pp. 36-38.

[6]. Kahn David, "Information Hiding-History of Steganography", Lecture notes in Computer Science, Springer, 2005, Vol. 1174, pp. 1-5.

[7]. Anderson, R. J., Petitcolas,: "On the limits of steganography", IEEE Journal of selected Areas in Communications, 1998, Vol. 16, pp. 474-481.

[8]. Ahsan Kamran, Kundur Deepa,: "Practical Data hiding in TCP/IP", Proceedings of the Workshop on Multimedia Security at ACM Multimedia, 2002.

[9]. Theodore G. Handel & Maxwell T. Sanford, "Hiding data in the OSI network model", Proceedings of the 1st International Workshop on Information Hiding, Springer, 1996, Vol. 1174, pp. 23-38.

[10]. Lee, K., Chen, L. H.: "High Capacity Image Steganographic Model", IEE Proceedings-Vision, Image and Signal Processing, 2000, Vol. 147, pp. 288-294.

[11]. Venkatraman, S., Abraham, A., Paprzycki, M.: "Significance of Steganography on Data Security", Proceedings of the International Conference on Information Technology: Coding and Computing, IEEE, 2004, Vol. 2, pp. 347-351.

[12]. Ni, Z., Shi, Y. Q., Ansari, N., Su, W.: "Reversible data hiding", IEEE Transactions on Circuits System Video Technology, 2006, Vol. 16, pp. 354–362.

[13]. Morkel, T., Eloff, J. H. P., Olivier, M. S.: "An Overview of Image Steganography", Proceedings of Information and Computer Security Architecture (ICSA) Research Group, Pretoria, South Africa, 2005, pp. 1-12.

[14]. Reference guide: "Graphics Technical Options and Decisions", http://www.devx.com/projectcool/Article/1997.

[15]. F.A.P. Petitcolas, Katzenbeisser, S.: "Information Hiding Techniques for Steganography and Digital Watermarking," Artech House, Inc., Boston, London, 2000, pp. 64-72.

[16]. Marvel, L. M., Boncelet, C. G. Retter, C.: "Spread Spectrum Steganography", IEEE Transactions on image processing, 1999, Vol. 8, pp. 1075-1083.

[17]. Mohamed A. Seif Eldeen, Abdellatif A. Elkouny, Salwa Elramly, "DES Algorithm Security Fortification using Elliptic Curve Cryptography", International Conference on Computer Engineering and Systems, IEEE, pp. 335-340, 2015.

[18]. Md. Rashedul Islam, Ayasha Siddiqa, "An Efficient Filtering based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography", International Conference on Inforamtics, Electronics and Vision, IEEE, pp. 1-6, 2014.

[19]. Kuang Tsan Lin and Sheng Lih Yeh, "Hiding a Covert Digital Image by Assembling the RSA Encryption Method and the Binary Encoding Method", Journal of Mathematical Problems in Engineering, Hindawi Publishing Corporation, Vol. 2014, pp. 1-8, 2015.

International Journal of Engineering Research and Applications (IJERA) is **UGC approved** Journal with Sl. No. 4525, Journal no. 47088. Indexed in Cross Ref, Index Copernicus (ICV 80.82), NASA, Ads, Researcher Id Thomson Reuters, DOAJ.

Poonam Yadav. "A Hybrid of Steganography and Cryptography for Decreasing Mean Square Error and Bit Error Rate ." International Journal of Engineering Research and Applications (IJERA) , vol. 7, no. 11, 2017, pp. 44–49.