

SECURE DATA TRANSMISSION USING STEGANOGRAPHY AND ENCRYPTION TECHNIQUE

Shamim Ahmed Laskar¹ and Kattamanchi Hemachandran²

Department of Computer Science
Assam University, Silchar, India

¹shamim.aus@rediffmail.com, ²khchandran@rediffmail.com

ABSTRACT

With the spread of digital data around the world through the internet, the security of the data has raised a concern to the people. Many methods are coming up to protect the data from going into the hands of the unauthorized person. Steganography and cryptography are two different techniques for data security. The main purpose in cryptography is to make message concept unintelligible, while steganography aims to hide secret message. Digital images are excellent carriers of hidden information. We propose a method of combining steganography and cryptography for secret data communication. In this paper, we propose a high-performance JPEG steganography along with a substitution encryption methodology. The approach uses the discrete cosine transform (DCT) technique which used in the frequency domain for hiding encrypted data within image. Experimental results show that the visual and the statistical values of the image with encrypted data before the insertion are similar to the values after the insertion thus reduces the chance of the confidential message being detected and enables secret communication. The effectiveness of the proposed method has been estimated by computing Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR).

KEYWORDS

Steganography, Cryptography, plaintext, encryption, decryption, ciphertext, substitution cipher, discrete cosine transform, JPEG, quantization, Mean square error and Peak Signal to Noise Ratio.

1. INTRODUCTION

In the digital world, data is the heart of computer communication and global economy. To ensure the security of the data, the concept of data hiding has attracted people to come up with creative solutions to protect data from falling into wrong hands [1]. Digital data can be delivered over computer networks from one place to another without any errors and interference. The distribution of digital media raised a concern over the years as the data are attacked and manipulated by unauthorized person [2]. Digital data can be copied without any loss in quality and content. Thus it poses a big problem for the security of data and protection of intellectual property rights of copyright owners [3]. The Internet provides a method of communication as a

means to distribute information to the masses. As a result of spreading of Internet around the world, motivation of hiding secret message in different multimedia and secure communication via Internet is increased [5]. Techniques for information hiding are increasing day by day with more sophisticated approach. The digital media which are used for secret communication includes text, images, audio and videos which provide excellent carriers for hidden information. Due to the growth of data communication over computer network, the security of information has become a major concern [4]. Thus to protect data from unauthorized access and use, the data confidentiality and integrity are required.

Steganography and cryptography are the two different information hiding techniques which provide confidentiality and integrity of data [8]. Steganography technique aims to transmit a message on a channel, where some other kind of information is already being transmitted [6]. The goal of steganography is to hide messages inside other “harmless” digital media in a way that does not allow any person to even detect the presence of secret message [4]. The main goal of steganography is to communicate securely in such a way as to avoid drawing suspicion to the transmission of a hidden data [7]. Cryptography hides the contents of a secret message from an unauthorized person but the content of the message is visible [4]. In cryptography, the structure of a message is scrambled in such a way as to make it meaningless and unintelligible manner [12]. Basically, cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it [11].

Steganography does not alter the structure of the secret message, but hides it inside a medium so that the change is not visible [7]. In other words, steganography prevents an unintended recipient from suspecting that the data exists and the security of the steganography system relies on secrecy of the data encoding system [1]. Once the encoding system is known, the steganography system is defeated. While cryptography protects messages from unauthorized individual by changing the meaning, steganography techniques enable concealment of the fact that a message is being sent through digital media. Steganography is the invisible communication between the sender and the receiver [14]. In Steganography, only the sender and the receiver know the existence of the message, whereas in cryptography the existence of the encrypted message is visible to the world [13]. For this reason, steganography removes the unwanted attention coming to the media in which the message is hidden [30].

Steganography and Cryptography are different in their way of data hiding but they are in fact complementary techniques. No matter how strong the encryption algorithm may be, if secret message is discovered, it will be subject to cryptanalysis [31]. Likewise, how well a message is concealed inside a digital media there is possibility of the hidden message to be discovered by the third party. By combining Steganography and Cryptography we can achieve better security by concealing the existence of an encrypted message [8, 9]. The resulting stego-object can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to detect the message from the stego-object, he at first have to decode the message from digital media and then he would still require the cryptographic algorithm to decipher the encrypted message [10].

2. IMAGE BASED STEGANOGRAPHY

All digital file formats can be used for hiding data using steganography, but the formats that have a high degree of redundancy present in them are more suitable. The redundant bits of an object

are those bits that can be altered without the alteration being detected easily [4, 16]. As digital images contain large volume of redundant bits, they are the most popular digital media for steganography. This is relatively easy because an image, being an array of pixels, typically contains an enormous amount of redundant information [6, 32]. An image is a collection of numbers that constitute different light intensities in different areas of the image. Image based steganography is about exploiting the limited powers of the human visual system (HVS) [5, 28]. There are many ways to hide messages within images. The security of stego-images depends entirely on their ability to go unnoticed [5].

When working with digital images, the images seems to be too large to be transmitted over the Internet. So, techniques are used to reduce the image size in order to display it in a reasonable time [24]. These techniques make use of mathematical formulas to analyze and reduce image data, resulting in smaller file sizes and the process is called compression [7]. Choice of the cover image is an important factor of steganographic technique and thus compression plays a vital role. Current image formats can be divided into two categories based on compression, lossy and lossless. Both methods save storage space but have different results. Lossless compression reconstructs the original message exactly and thus it is preferred when the original information must remain intact [15, 16]. Lossless images are more suitable for embedding, since the integrity of the image data is preserved. However, they do not have high compression ratio as lossy formats do. Lossy compression, on the other hand, saves space but may not maintain the original image's integrity. The plus side of lossy images, in particular JPEG, is that it achieves extremely high compression, while maintaining fairly good quality [16, 17]. Previously, it was felt that steganography using JPEG images is not possible as lossy compression involves reduction of bits and thus data may be lost [4]. One of the major characteristics of steganography is the fact that information is hidden in the redundant bits of an object and since redundant bits are left out when using JPEG it was feared that the hidden message would be destroyed [14]. However, the properties of the compression algorithm have been exploited in order to develop a steganographic algorithm for JPEGs [18]. Thus it is not necessarily perceptible to a human eye that the image has been changed [20]. Lossy compression is preferred in image based steganography because it achieve higher compression compared to lossless compression and thus it is much more secure and have less chances of detection that that of lossless. Steganography not only deals with embedding the secret data inside the digital image but also the receiver to whom the message is intended must know the method used and would be able to retrieve the message successfully without drawing the attention of a third party that a secret communication is occurring.

3. BACKGROUND OF THE PROPOSED TECHNIQUE

Cryptography is the method of encoding or scrambling secret messages whose meaning cannot be understood by others who try to intercept the message [31]. The purpose of cryptography is to protect the secret message from unintended receiver or attacker. Unless the technique of the encoding system is known, the data cannot be retrieved. A Cryptographic algorithm is considered computationally secure if it cannot be broken with available resources [30]. The technique for deciphering cipher messages is called cryptanalysis which signifies that the set of methods for obtaining the meaning of encrypted information [11]. Successful cryptanalysis may recover the plaintext or the key by finding weaknesses in the cryptosystem that would lead to an attack from a third party [27].

Steganography is the method of hiding confidential messages into digital media in a way that no one apart from the sender and intended receiver even realizes there is a hidden message inside the media [1]. Steganography techniques are used to address digital rights, information security and conceal secrets. Most of the steganographic systems in the present days use images as cover media because digital images are mostly transmitted over Internet communication [7]. Digital images often have a large amount of redundant data or noise present in them and this provides space to embed data and the modification in the image is not perceptible to a human eye [16]. Steganalysis is a term closely related to steganography which is a method for detecting hidden messages in digital medium [6]. Today advances in steganography are followed by advances in steganalysis. Image based steganographic methods aims to make changes not detectable by the human eye. This feature is not enough because statistical methods can detect the changes in the image even if it is not visible [20]. Compression also plays a vital role in image based steganography because the outcome of the steganographic technique depends on the compression scheme used [17]. Steganographers are trying to find more efficient method of embedding message in a digital file, only to get rid of being defeated by techniques derived by steganalysts.

Existing cryptographic systems only provide privacy and confidentiality but they don't have a component to conceal cryptographic communication. Under certain conditions steganography can be used for data security as it enables invisible communication, but steganography, like cryptography, can be detected [6]. Hence our approach is to transfer some features of steganography to cryptography, rather than use steganography itself. Neither cryptography nor steganography alone is a good solution to information security, but their combination can provide very good method of data security [8]. When the secret message which is to be transmitted is first encrypted using cryptographic algorithm and then embedded into the frequency domain of an image using steganography, the expected security of the secret data can be raised. Steganography and cryptography differ in their way of data hiding. The aim of the present work is to devise a model holding the features of steganographic and cryptographic model by integrating cryptography and steganography through image processing [9]. The combining model will result a steganographic one and will perform cryptographic functionality and, preserving its steganographic nature [10].

Different algorithms offer different levels of security of data and it depends on how difficult the algorithm is to break. The secret data is supposed to be safe if the cost of breaking the algorithm is greater than the value of the secret data and also if the time required in breaking an algorithm is longer than the time the information must remain secret.

4. PROPOSED TECHNIQUE

In this paper we propose a technique of combining cryptography and steganography to solve the problem of unauthorized data access. Steganography also can be implemented to cryptographic data so that it increases the security of this data [8, 9]. In this method we first encrypt a message using substitution cipher method and then embed the encrypted message inside a JPEG image using DCT in frequency domain. A substitution cipher is one in which each character in the plaintext is substituted for another character in the ciphertext [31]. Thus the content of the message appears meaningless to the third party. Thus it is very difficult to detect hidden message in frequency domain and for this reason we use transformation like DCT in our proposed technique. The combination of these two methods will enhance the security of the data embedded and will satisfy the requirements such as capacity, security and robustness for secure data

transmission over an open channel [10]. Furthermore, if an attacker were to defeat the steganographic technique to detect the message from the stego-object, he would still require the cryptographic method to decipher the encrypted message [8]. The intended receiver should be able to recover the embedded data successfully, without any errors.

4.1. Encrypting message

Substitutions and transpositions encryption are regarded as the building blocks of Classical cryptography technique [31]. A transposition cipher hides information by reordering the letters of the message. In a transposition cipher the plaintext remains the same, but the order of characters is shuffled around [13]. Thus the frequency analysis on the ciphertext would reveal that each letter has approximately the same [11]. A substitution cipher is one in which each character in the plaintext is substituted for another character in the ciphertext [13]. A substitution cipher is an encryption scheme that uses only substitution transformations. The two other techniques related with transposition and substitution for obscuring the redundancies in a plaintext message are diffusion and confusion [30]. Diffusion dissipates the redundancy of the plaintext by spreading it out over the ciphertext. The simplest way to cause diffusion is through transposition. Confusion obscures the relationship between the plaintext and the ciphertext. The easiest way to do this is through substitution. In the proposed method substitution encryption method is used. The orders of the letters are changed in transposition cipher, whereas in substitution cipher the letters are replaced with other letter so as to make the message unintelligible [26]. In substitution cipher, the algorithm is to offset the alphabet and the key is the number of characters to offset it [31]. The receiver inverts the substitution on the ciphertext to recover the plaintext [25]. For example, if we encrypt the word “MESSAGE” by shifting 18 places, then “CRYPTOGRAPHY” encrypts as “UJQHLGYJSHZQ”. To allow someone else to read the ciphertext, we tell the recipient that the key is 18. Now if we suppose A (sender) wants to send B (recipient) the plaintext message M over the insecure communication line, A encrypts M by computing the ciphertext $C = E(K, M)$ and sends C to B. Upon receipt, B decrypts C by computing $M = D(K, C)$. The adversary may know E and D are the encryption and decryption algorithms respectively which are being used in the process.

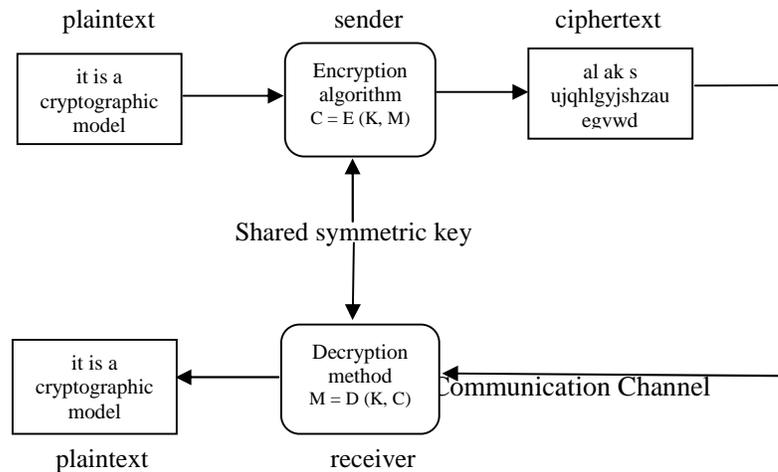


Fig 1: Symmetric encryption system

- *Plaintext*: It is the original message which is to be transmitted. It can be written as $M = \langle m_1, m_2, \dots, m_n \rangle$ to denote the plaintext. For example, $M = \langle t, h, i, s, , i, s, , a, n, , e, n, c, r, y, p, t, i, o, n, , m, e, t, h, o, d \rangle$.
- *Ciphertext*: It is the translated or encrypted message, which can be denoted as $C = \langle c_1, c_2, \dots, c_m \rangle$. Thus, the ciphertext $C = \langle j, x, y, i, , y, i, , q, d, , u, d, s, h, o, f, j, y, e, d, , c, u, j, x, e, t \rangle$.
- *Encryption*: The process of transformation from plaintext to ciphertext. The encryption is denoted using $C = E(M)$, where C is the ciphertext and M is the plaintext and E is the encryption method. In the present substitution method, $C = E(M) = (M + 16) \bmod (26)$; in general, $C = E(M) = (M + K) \bmod (26)$, where K is the key.
- *Decryption*: It is the reverse process of encryption which is the transformation from ciphertext to plaintext, formally denoted as $M = D(C)$. In the present substitution method, $M = D(C) = (C - 16) \bmod (26)$; in the general, $M = D(C) = (C - K) \bmod (26)$, where K is the key.
- *Key*: Key is the agreement between the sender and the recipient. In the present encryption method the key tells how much to shift. It is an input to the encryption and decryption algorithm [31]. The encryption algorithm will produce a different ciphertext depending on the specific key being used. The corresponding key is needed to decrypt the ciphertext to plaintext [27]. A key gives us flexibility in using an encryption algorithm and provides additional security [19]. When same key used for encryption and decryption as shown in Fig. 1, they are called *symmetric key*, or *secret key* [19]. The encryption process can be denoted as $C = E(K, M)$; and the decryption process is denoted as $M = D(K, C)$. The cryptosystem is called *symmetric cryptosystem* and needs to satisfy $M = D(K, E(K, M))$.

4.2. Embedding the encrypted message in image file

Images are the most popular cover objects for steganography because of large amount of redundant bits which are suitable for data transmission on the Internet [24]. An example of an image format that uses this compression technique is JPEG (Joint Photographic Experts Group) [17]. JPEG is the most popular image file format on the Internet and the image sizes are small because of the compression, thus making it the least suspicious algorithm to use. The JPEG format uses a discrete cosine transform to image content transformation. DCT is a widely used tool for frequency transformation [23].

The working method of Steganography in DCT is discussed as follows. In order to compress an image into JPEG format, the RGB colour representation is first converted to a YUV representation space and break up each colour plane into 8×8 blocks of pixels [18, 21]. In this representation the Y component corresponds to the luminance (or brightness) and the U and V components correspond to chrominance (or colour) [22, 23]. The human eye is more sensitive to changes in the brightness (luminance) of a pixel than to changes in its colour. Thus it is possible to remove a lot of colour information from an image without losing a great deal of quality [17]. The fact is exploited by the JPEG compression by down sampling the colour data to reduce the size of the file. The colour components (U and V) are halved in horizontal and vertical directions, thus decreasing the file size by a factor of 2.

The next step is the actual transformation of the image. The DCT transforms [20] a signal from an image representation into a frequency representation, by grouping the pixels into 8×8 pixel blocks and transforming the pixel blocks into 64 DCT coefficients each [22]. A modification of a single

DCT coefficient will affect all 64 image pixels in that block. Discrete cosine transformations (DCT) are used by the JPEG compression algorithm to transform successive 8 x 8 pixel blocks of the image, into 64 DCT coefficients each [24]. Each DCT coefficient $F(u, v)$ of an 8 x 8 block of image pixels $f(x, y)$ is given by:

$$F(u, v) = \frac{1}{4} C(u)C(v) \left| \sum_{x=0}^7 \sum_{y=0}^7 f(x, y) \cos \frac{(2x+1)u}{16} \cos \frac{(2y+1)v}{16} \right| \quad (1)$$

$$\text{where } C(u) = 1/\sqrt{2} \text{ when } u=0 \text{ and } C(u)=1 \text{ otherwise.}$$

$$C(v) = 1/\sqrt{2} \text{ when } v=0 \text{ and } C(v)=1 \text{ otherwise.}$$

Having the data in the frequency domain allows the algorithm to discard the least significant parts of the image. The JPEG algorithm does this by dividing each cosine coefficient in the data matrix by some predetermined constant, and then rounding up or down to the closest integer value [21]. The next step is the quantization [17] phase of the compression. The aim is to quantize the values that represent the image after transforming values to frequencies [22]. Quantization is the process of taking the 64 DCT coefficients and dividing them individually against a predetermined set of values and then rounding the results to the nearest real number value [6, 18]. The human eye is fairly good at spotting small differences in brightness over a relatively large area, but not so good as to distinguish between different strengths in high frequency brightness [23]. This means that the strength of higher frequencies can be diminished, without changing the appearance of the image. JPEG does this by dividing all the values in a block by a quantization coefficient [22].

After calculating the coefficients, the following quantizing operation is performed:

$$F^Q(u, v) = \left\lfloor \frac{F(u, v)}{Q(u, v)} \right\rfloor \quad (2)$$

where $Q(u, v)$ is a 64-element quantization table.

The encrypted message bits are embedded into the DCT coefficients in the quantization phase. DCT coefficients transform an image from the spatial domain to the frequency domain. DCT is used in image steganography is broken into 8x8 blocks of pixels and is applied to each block [18]. Each block is compressed through quantization table to scale the DCT coefficients and encrypted message is embedded in quantized DCT coefficients. The selected coefficients after quantization are ordered by magnitude and then modified by the corresponding bit in the message stream. The quantization step is lossy because of the rounding error [22]. The quantized coefficients are then passed to the entropy encoding step to form the compressed code.

After quantization, zigzag type motion is performed to group similar frequencies together. Zigzag ordered encoding collects the high frequency quantized values into long strings of zeros [21]. In zigzag small unimportant coefficients are rounded to 0 while larger ones lose some of their precision [18]. To perform a zigzag encoding on a block, the algorithm starts at the discrete cosine value and begins winding its way down the matrix. This converts an 8 x 8 table into a 1 x 64 vector. The results are rounded to integer values and the coefficients are encoded using Huffman coding to further reduce the size [17]. Huffman coding scans the data being written and assigns fewer bits to frequently occurring data, and more bits to infrequently occurring data [23]. The size

field for discrete cosine values is included in the Huffman coding for the other size values, so that JPEG can achieve even higher compression of the data.

Thus it is important to recognize that the JPEG compression algorithm is actually divided into lossy and lossless stages [7]. The DCT and the quantization phase form part of the lossy stage, while the Huffman encoding used to further compress the data is lossless. Steganography can take place between these two stages [14]. Using this principle of insertion the encrypted message can be embedded into DCT coefficients before applying the Huffman encoding [17]. By embedding the information at this stage, in the transform domain, it is extremely difficult to detect, since it is not in the visual domain [18]. Transform embedding methods are found to be in general more robust than other embedding methods which are susceptible to image-processing type of attacks [23].

5. EXPERIMENTAL ANALYSIS

The proposed method was experimented using MATLAB. The plaintext is first encrypted to generate the ciphertext using substitution cipher method. A key is used in the encryption which is based on symmetric cryptosystem where same key is used for both encryption and decryption process. Then the ciphertext is embedded inside the JPEG image file using DCT technique that embeds the information in the frequency domain. The generated stego-image is sent over to the intended recipient. The whole idea of the proposed method is to model a technique that enables secure data communication between sender and receiver. By this approach the messages were successfully embedded into the cover images. In the experiment messages of different sizes were successfully embedded into different set of images ranging from 30 KB to 400 KB. In the method of retrieval the message is first extracted from the stego-image. The message is then decrypted by producing the key used in encryption to get back the original message. If the key does not match the original information will remain unreadable.



a



b

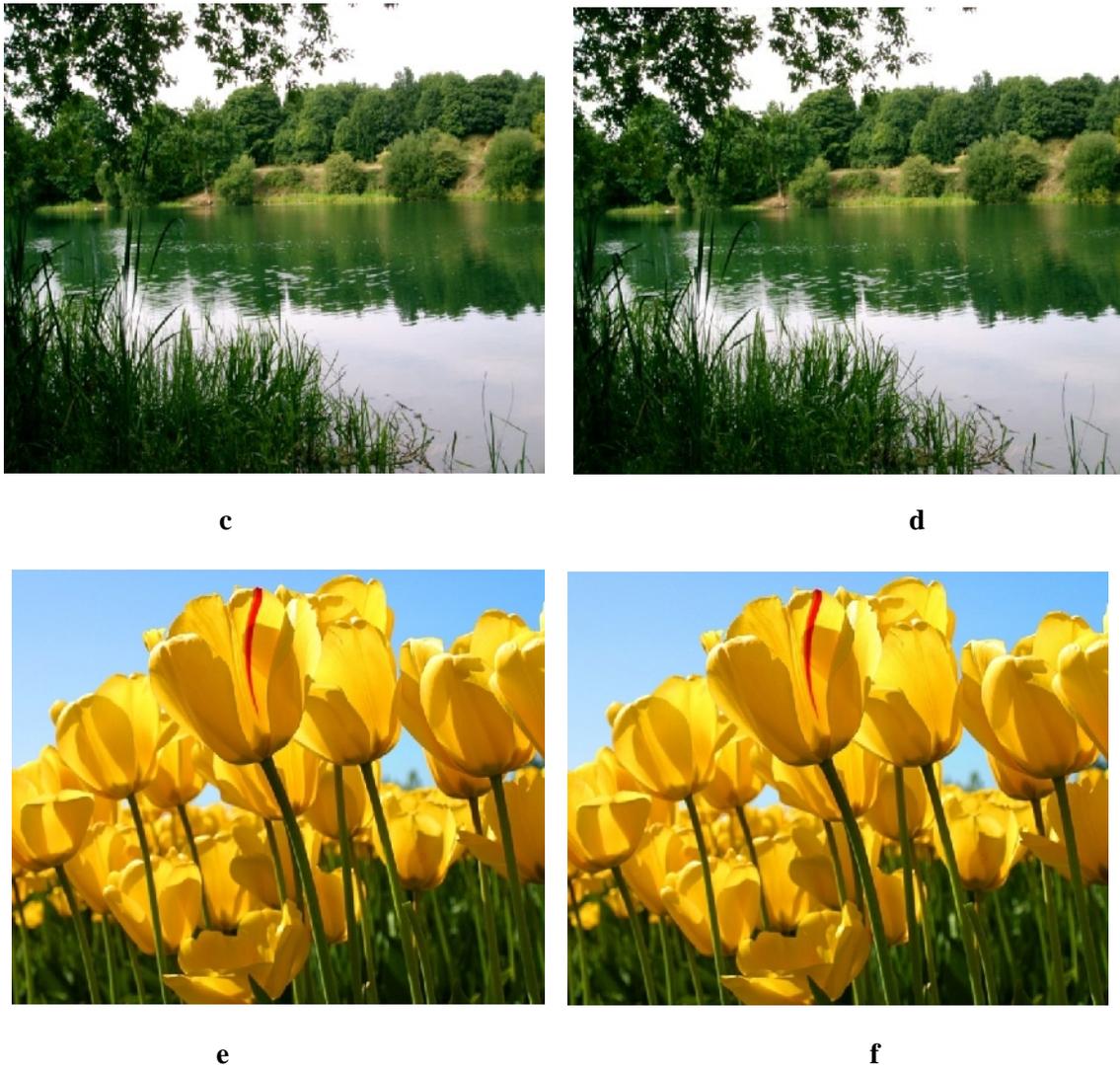


Fig. 2. flower (a) Original image (b) stego image *lake* (c) Original image (d) stego image, *tulip* (e) Original image (f) stego image.

The messages that were embedded into the images were extracted successfully. It is observed that the human visual system (HVS) cannot distinguish the cover-image and stego image [28] the complexity of the image is not disturbed as shown in figure 2 (a) and (b), (c) and (d), (e) and (f). The work not only aims to preserve the visual integrity of the image used for embedding but also the method should be free from statistical attacks because with the advances in steganalysis technique various statistical methods can detect modification in image bits. So, distortion analysis of stego images is carried out by studying distortion / similarity statistically. Distortion between two different images is measured by considering Mean Square Error (MSE), and PSNR (peak signal to noise ratio) [29].

The invisibility of the hidden message is measured in terms of the Peak Signal-to-Noise Ratio [28]. To analyze the quality of the embedded texture image, with respect to the original, the measure of PSNR has been employed [29]:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (3)$$

where mean square error (MSE) is a measure used to quantify the difference between the cover image I and the stego (distorted) image I' [28]. If the image has a size of $M * N$ then

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N [I(i, j) - I'(i, j)]^2 \quad (4)$$

TABLE 1. MSE and PSNR values for the Original and Stego images

Cover image	Stego Image	No. of bytes embedded	MSE %	PSNR (dB)	No. of bytes extracted
flower	steg_flower	1560 bytes	2.74	43.75	1560 bytes
lake	steg_lake	1816 bytes	3.34	42.88	1816 bytes
tulip	steg_tulip	2676 bytes	4.88	41.24	2676 bytes

It has been observed that when the payload increases, the MSE increases, and this affects the PSNR inversely [23]. So, from trade-off it was found that MSE decrease causes PSNR increase and vice-versa. PSNR is often expressed on a logarithmic scale in decibels (dB). PSNR values falling below 30 dB indicate a fairly low quality, i.e. distortion caused by embedding can be obvious. However, a high quality stego-image should strive for 40 dB and above [28]. Our results indicate that embedding process introduces less perceptual distortion and higher PSNR [29]. It is to be noted that PSNR ranging from 41 dB to 43 dB means that the quality degradations could hardly be perceived by a human eye.

6. CONCLUSION

In this paper an attempt has been made to identify the requirements of a good data hiding algorithm and the technique has its place in secure data communication. Steganography is the data hiding technique which comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to obscure the very existence of the embedded data. Neither Steganography nor cryptography alone is a good solution for data secrecy from the attacks. But if these methods are combined, the system may provide more security to the data. If a message is encrypted and hidden with a steganographic method, it provides an additional layer of protection and reduces the chance of the hidden message being detected. This combinational methodology will satisfy the requirements such as capacity, security and robustness for secured data transmission over an open channel. These combined techniques can be propelled to the forefront of the current security techniques by the remarkable growth in computational power, the increase in security awareness among the individuals, groups, agencies, government organization

and through intellectual pursuit. Here we embed the confidential message into an image file in such a manner that the degradation in quality of the carrier image is not noticeable. Thus the proposed method allows users to send data through the network in a secured fashion and it can be employed for applications that require high-volume embedding with robust against attacks. The steganography method may be further secured if we compress the secret message first and then encrypt it and then finally embed inside in the cover image.

ACKNOWLEDGEMENTS

One of the authors (Shamim Ahmed Laskar) gratefully acknowledges UGC for granting Research fellowship (Maulana Azad National Fellowship).

REFERENCES

- [1] M. Conway, "Code Wars: Steganography, Signals Intelligence, and Terrorism", Knowledge Technology & Policy, Volume 16, Number 2, pp. 45-62, Springer, 2003.
- [2] R. J. Anderson and F. A. P. Petitcolas, "On The Limits of Steganography", IEEE Journal of Selected Areas in Communications, 16(4), pp.474-481, May 1998, ISSN 0733-8716.
- [3] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information Hiding-A Survey", Proceedings of the IEEE, 87(7), pp.1062-1078, July 1999.
- [4] S. A. Laskar and K. Hemachandran, "An Analysis of Steganography and Steganalysis Techniques", Assam University Journal of Science and Technology, Vol.9, No.II, pp.83-103, January, 2012, ISSN: 0975-2773.
- [5] C. Hosmer, "Discovering Hidden Evidence", Taylor & Francis Group, Journal of Digital Forensic Practice, Vol. No.1, pp.47-56, 2006.
- [6] B. Li, J. He, J. Huang and Y. Q. Shi, "A Survey on Image Steganography and Steganalysis", Journal of Information Hiding and Multimedia Signal Processing, Vol. 2, No. 2, pp. 142-172, April, 2011, ISSN 2073-4212.
- [7] N.F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE, Computer, vol. 31, no. 2, pp. 26-34, Feb. 1998.
- [8] A. J. Raphael and V. Sundaram, "Cryptography and Steganography – A Survey", Int. J. Comp. Tech. Appl., Vol 2 (3), pp. 626-630, ISSN:2229-6093.
- [9] S. Song, J. Zhang, X. Liao, J. Du and Q. Wen, "A Novel Secure Communication Protocol Combining Steganography and Cryptography", Elsevier Inc, Advanced in Control Engineering and Information Science, Vol. 15, pp. 2767 – 2772, 2011.
- [10] M. A. Fadhil, "A Novel Steganography-Cryptography System", Proceedings of the World Congress on Engineering and Computer Science 2010, USA, Vol. I, October, 2010, ISSN: 2078-0966.
- [11] R. Anderson, "Cryptanalytic Properties of Short Substitution Ciphers", Taylor & Francis, Cryptologia, Vol. XIII, No. 1, pp. 61-72, January, 1989.
- [12] G. J. Simmons, "Subliminal Channels: Past and Present," European Transactions on Telecommunications, Vol. 4, No. 4, pp. 459-473, Aug 1994.
- [13] R. S. Ramesh, G. Athithan and K. Thiruvengadam, "An Automated Approach to Solve Simple Substitution Ciphers", Taylor & Francis, Cryptologia, Vol. XVII, No. 2, pp. 202-218, April, 1993.
- [14] E. Walia, P. Jain and Navdeep, "An Analysis of LSB & DCT based Steganography", Global Journal of Computer Science and Technology, Vol. 10 Issue 1 (Ver 1.0), pp 4-8, April, 2010.
- [15] M. Kaur, S. Gupta, P. S. Sandhu and J. Kaur, "A Dynamic RGB Intensity Based Steganography Scheme", World Academy of Science, Engineering and Technology 67, pp 833-836, 2010.
- [16] P. Khare, J. Singh and M. Tiwari, "Digital Image Steganography", Journal of Engineering Research and Studies, Vol. II, Issue III, pp. 101-104, July-September, 2011, ISSN:0976-7916.

- [17] A. B Watson, "Image Compression Using the Discrete Cosine Transform", *Mathematica Journal*, 4(1), pp. 81-88, 1994.
- [18] C-L Liu and S-R. Liao, "High-performance JPEG steganography using complementary embedding strategy", Elsevier Inc, *Journal of Pattern Recognition* Vol. 41, pp.2945 – 2955,2008.
- [19] B. B. Zaidan, A. A. Zaidan, A.K. Al-Frajat and H.A. Jalab, "On the Differences between Hiding Information and Cryptography Techniques: An Overview", *Journal of Applied Sciences*, Vol.10, No.15, pp.1650-1655, 2010.
- [20] M. Kharrazi, H. T. Sencar and N. Memon, "Performance study of common image steganography and steganalysis techniques", *Journal of Electronic Imaging*, SPIE Proceedings Vol. 5681.15(4), 041104 (Oct–Dec 2006). SPIE and IS&T., 2006.
- [21] B.J. Erickson, "Irreversible Compression of Medical Images", *Journal of Digital Imaging*, Vol. 15, No.1, pp. 5-14, March, 2002.
- [22] A. B. Watson, "Perceptual Optimization of DCT Color Quantization Matrices", *Proceedings of the IEEE International Conference on Image Processing*, Austin, TX, Nov., 1994.
- [23] X. Li and J. Wang, "A steganographic method based upon JPEG and particle swarm optimization algorithm", *Information Sciences* 177 (15) (2007) 3099–31091.
- [24] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography", *IEEE Security and Privacy*1(3) pp. 32–44, 2003.
- [25] S. Ravi and K. Knight, "Attacking Letter Substitution Ciphers with Integer Programming", Taylor & Francis, *Cryptologia*, Vol.33, No.4, pp.321-334, 2009.
- [26] P. Kaijser, T. Parker, and D. Pinkas, "SESAME: The Solution to Security for Open Distributed Systems," *Journal of Computer Communications*, Vol. 17, No. 4, pp. 501-518, Jul 1994.
- [27] G.W. Hart, "To Decode Short Cryptograms," *Communications of the ACM*, Vol. 37, No. 9, pp. 102-108, Sept 1994.
- [28] B. E. Carvajal-Gómez , F. J. Gallegos-Funes and J. L. López-Bonilla, "Scaling Factor for RGB Images to Steganography Applications", *Journal of Vectorial Relativity*, Vol.4, No.3 pp.55-65, 2009.
- [29] G. Ulutas , M. Ulutas and V. Nabyev, "Distortion free geometry based secret image sharing", Elsevier Inc, *Procedia Computer Science*, Vol.3, pp.721–726, 2011.
- [30] W.F. Friedman, "Cryptology," *Encyclopedia Britannica*, Vol. 6, pp. 844-851, 1967.
- [31] Atul Kahate, "Cryptography and Network Security", 2nd Edition, Tata McGraw-Hill, 2008.
- [32] R. C. Gonzalez and R. E. Woods, "Digital Image Processing", 2nd edition, Prentice Hall, Inc, 2002.

Authors

Shamim Ahmed Laskar received his B.Sc. and M.Sc. degrees in Computer Science in 2006 and 2008 respectively from Assam University, Silchar, where he is currently doing his Ph.D. His research interest includes Image Processing, Steganography, Information Retrieval and Data Security.



Prof. Kattamanchi Hemachandran obtained his M.Sc. Degree from Sri Venkateswara University, Tirupati and M.Tech and Ph.D Degrees from Indian School of Mines, Dhanbad. Presently, he is serving as Head, Department of Computer Science, Assam University, Silchar. He is associated with this department since 1998. He is supervising many research scholars. His areas of research interest are Image Processing, Software Engineering and Distributed Computing.

