A Novel Modified Play-Fair Image Steganography by Using 9 by 4 Matrixes

Sandeep.y, K.A.Naveen Kumar, G.Reddy Gangadri

ABSTRACT: From recent years the rapid growth in usage of internet increases where it plays asubstantial role in sharing the information i.e., audio, video, data. Sometimesthis information is observant by the unwanted persons and it is stolen over the internet before it is transmitted. So the message has to be secured over the travel between the users. Miserably it is not enough to preserves the content of the ambiguous information but also the entity of the information. In this paper we approach a technique called steganography where the modern data compression, spread spectrum and cryptography all get together to satisfy the privacy requirement. In this paper the information is hided in a cover media and encrypted using Play-Fair algorithm by using 9X4 matrix. The information has to be encrypted under the cover image which is known to be stego-image. Now the image is compressed and sends to the user. At the receiver end the stego-image is decompressed and the information is decrypted from the image. The information is transferred more securely over the stego-image and the need of privacy is satisfied by using Play-Fair algorithm.

Index Terms: Cryptography, Data Compression, Decryption, Encryption,Play-Fair Steganography, Privacy, Spread Spectrum, and Stego-image.

1. Introduction

The most substantial consideration for information technology and communication is sudden raise in the usage of internet for the transmission of information between the users. They are different factors which play a substantial role in the transmission of information over the internet. So the information should be transferred with more privacy, fastly, error freely. To improve the needof privacy for the users several techniques have been implemented.Among several techniquesone of the best techniques that can be implemented is cryptography. Miserably it is not only enough to preserve the content of the ambiguous information but also the existence. The technique which is mainly used for the existence is known as Steganography [1]. Steganography mainly refers to the science of invisible communication. The word steganography is derived from Greek word and the main principle of steganography is 'cryptic writing' in which the data is cryptic in a cover media so that the data cannot be noticed by others in the transmission. The encapsulated data is the message which it has to be sending ambiguously where it can be done by using image file or it can be an audio file. The file which used to cover the message is known as cover-file, cover-image or cover-audio. The combination of both messages with image forms the stego-object.

The main substantial factor that should be considered that what type of image is preferred as the cover-image. Images which are accommodate with a minimum number of colors, computer art, images which are having a unique semantic content are not preferable to be a cover image. Some substantial experts recommended gray scale images can act as a best cover images where the data is hidden more securely. Uncompressed scans of photographs or images which are obtained with a digital camera may accommodate with high number of colors and these types of images are

Sandeep.y, AssistantProfessor at MTIET Palamaner,ph:+919502818656, ysreddy.210@outlook.com.
K.A.Naveen Kumar, Assistant Professor at MTIET Palamaner, ph:+918008997541,Naveen.k.86@gmail.com.
G.Reddy Gangadri, seating assistant at MTIET, Palamaner, ph: +919959132682, gangadhar.reddy482@gmai.com

IJSER

usually recommended and these types of images are considered more secure and safe.

Cryptography helps in protecting the content of messages whereas the steganography helps in concealing the existence [2]. If the message is cryptic in the image and then encrypted at the receiver end the same image has to be decrypted, which can provide another layer of protection which helps in improving the privacy need. The expected features of a stego-medium are that it can be more robustness and imperceptibility.The ambiguous message should be known only by the intended receiver and the stego-medium should able to withstand the attacks by intruder as the key which helps in decrypting the message is only known by the receiver.The characters of the ambiguous message encapsulated should have a protocol that it should not reduce the peculiarity of the stego image.

Key protocols that should be mainly considered when creating a digital data hiding system for the purpose of the effective steganography are:

Security of cryptic data: In order to avoid raising the distrustful of eavesdroppers, while evading the conscientious screening of algorithm detection, the cryptic contents must be concealed in terms of both perceptually and statistically.

Embedding Capacity: peculiarity of the image plays a very vital role, so the amount of ambiguous information that can be encapsulated without degrading the peculiarity of the image.

The paper is organized as follows: Section 2 reviews related to literature survey; Section 3 describes the existing Play-Fair technique; Section 4 describes the proposed Play-Fair technique followed by the algorithm for Play-Fair algorithm; finally Section 5 presents the conclusion.

2. Literature Survey

Steganography is the combination of cover medium and the secret message along with the stego key. This stego key mainly used to control the hiding process without any detection to unwanted parties which makes the features of steganography more robustness and imperceptibility. they are several steganography methods present they are

2.1 Pure steganography: where there will be no stego key will be present in the transmission of information. It is mainly based on the hypothesis that the communication is not aware by the intruder.

2.2 Secret key steganography: In this technique where the stego key is been exchanged between the users for the prior communication. This technique is most exposed to interception.

2.3 Public key steganography:In this technique both public key and the private key is been exchanged for the secure communication between the users and these public key can be break-in by the third party where as the private key is maintained and exchanged more ambiguously only between the users.

Basically steganography can be divided into many classifications

a. Spatial domain techniques
b. Transform domain techniques
c. Statistical techniques
d. Distortion techniques

a. Spatial Domain:

The pixel gray levels along with their color values have been used in this technique for encoding the message bits directly into the image.Spatial domain has a special advantage and simplest scheme compared to other algorithms in terms of

twain embedding and extraction.The considerable disadvantage of this algorithm isthat the quantity of additive noisethat crawl along with the image which exactly affects the statistical properties and the peak signal to noise ratio of the image which has the information present in it. Moreover these embedding algorithms are mainly helpful and applicable only to the lossless image-compression proposal like TIFF images and for lossy compression proposal like JPEG where these schemes are not that much predictable because some of the message bits may get lost along with the compression steps which may reduce the peculiarity of the transmission.

The are several schemes which belongs to this spatial domain in which one among them is Least Significant Bit (LSB) where the message bit representation is mainly done by the binary representation of the pixel gray levels. This approach of embedding scheme leads to an addition of a noise 0.5p in the pixel of the image where p represents the embedding rate in bits/pixel. This method of embedding rate can also supremacy to an asymmetry and also helps in grouping the different pixel gray values (0,1); (2,3); ….(254,255). To overcome this undesirable asymmetry, the adjustment is done in changing the least significant bit in which it is randomized and this technique is popularly known as Least Significant Bit (LSB) matching. By this kind of embedding it can be observed that it can add a noise of 0:5p on average and to decrease the value of noise [3] have approached the usage of binary function as two cover pixels where it helps to embed the data bits.

In mamtajuneja et.al.[4] scrutinize paper proposed an algorithm based on secured way of information security. It commenced with two component based LSB techniques for embedding the ambiguous data in the LSB's of blue and partial green elements of random pixel locations which are present at the edges of images. The algorithm is more flourishing as it is combined with a method known as Advanced Encryption Standards (AES).

In P.Thiyagarajan et.al.[5] scrutinize paper proposed a new immense capacity steganography algorithm which is mainly based on 3D geometric models.A part of triangular mesh is re-triangulated by the algorithm and a new triangular mesh positions are located. The ambiguous information is encapsulated into this newly formed triangular mesh. The vertices of the new triangular mesh are used for the embedding of the data. This algorithm is more withstand against many uniform affinetransformations which are likely to be cropping, rotation, and scaling.

In Shamim Ahmed Laskar et.al.[6] scrutinize paper proposed a technique of embedding data into red plane of the image. The algorithm mainly targets on increasing the security of the message and it also helps in reducing distortion rate. A PRNG is used to generate the stego key for the selection of pixel locations.

In S.ShanmugaPriya et.al.[7] scrutinize paper proposed a peculiar technique which is mainly based on LSB. The data embedding is accomplished by using a pair of pixels as a unit, where the first pixel of LSB carries only one bit of information and another function of two pixel values carriers another bit of information. Embedding is mostly done in a manner that shaper edge region are mainly uses the value of threshold value. The algorithm shows better performance not only in terms of distortion but also resistance against many existing steganalysis.

The main point that should be observed in spatial domain is that most of the approaches which are proposed here are mainly based on the minimization of the noise encapsulated in the cover. Another direction of the present steganography technique is to maintain the statistics of the image which may alter due to embedding.

IJSER

b. Transform Domain:

These algorithms attempt to encode message bits by the method using transform domain coefficients of the image and these are widely used for robust watermarking. Similar transform techniques include Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT). By embedding the data by using transform domain, the cryptic resides in more robust areas and spread across the entire image which makes the algorithm to provide better resistance against signal processing.

In Hemalatha.S et.al.[8] scrutinizer proposed a novel technique which uses two gray scale images which are of size 128 x 128 which can also be used as ambiguous image and embedding is done in RGB and $ycbcr$ domains. The algorithm uses Integer Wavelet Transform (IWT) method which helps in hiding the ambiguous data in the color cover images. The peculiarity of service of the stego images is good in RGB domain by comparing with the other PSNR values.

In Keith.L. Haynes et.al.[9] scrutinize paper proposed a novel technique which will make use of computer vision and machine learning techniques to get outcome where the message cannot be undetectable and if any intercepted occurred in the transmission it cannot be decrypted without key compromise. As to avoid thedetection the algorithm uses DWT. The main aim of a computer vision system is to allow machines to analyze the entire image and make a decision according to the content of that image. By the usage of this algorithm the security is been added to the encryption.

c. Statistical Techniques:

In Tomas Filler et.al.[10] scrutinize paper proposed a novel technique which helps for minimizing the presence of additive distortion in steganography with general embedding technique. The algorithm uses the Syndrome-Trellis Codes (STC) method as to improve the privacy of the system. STC separate the present samples into many different bins which uses as a common tool which helps for solving many information-theoretic and also the data-hiding problems. This proposed algorithm can also be used in both Spatial and Transform domain.

In Jessica Fridrich et.al. [11] Proposes a reversible embedding algorithm for VQ-compressed images which are mainly based on side matching and relocation. VQ (Vector Quantization) is a compression technique which makes the algorithm simpler in both encoding and decoding procedures which makes the algorithm more popular. The most earlier techniques achieves reversibility without using the location map so, even a small distortion of the original content is not applicable in some sensitive applications.

d. Distortion Techniques:

In M.B. OuldMedeni et.al. [12] Proposes a usage of error correcting codes in stenographic protocols. The algorithm referred to matrix encoding which have a protocol that both the sender and recipient have to agree in advance on parity check matrix H. The cover medium is processed to extract a sequence of v symbols, which arethen modified into s and these modified symbols help to embed the message m, sometimes s is alsoknown as thestego-data and the modifications on s are been translated on the cover-medium as to obtain the stego-medium.

In D.P.Gaikwad et.al.[13] proposes an image restoration technique in steganography. Where the algorithm uses a technique in which the image is blurred before hiding the message and algorithm uses point spread function and randomly generated key for hiding the message. The parameters used for blurring with PSF are used as keys which help in during the de-blurring. The ambiguous key which are generated by the algorithm are sending through the secure channel

IJSER

and these ambiguous key helps in decoding the ambiguous data.

3. Play-Fair Algorithm

Substitution ciphers are probably the most commonly used in the form of cipher. This mainly works by replacing each letter of the plain textwith another letter or sometimes it compensates with punctuation marks or with the spaces.

A monoalphabetic substitution cipher which may be known as the simple substitution cipher, which relies on a fixed substitute structure. That is, the substitution method may always fixed for eachletter of the alphabet in the information that that to be encrypted. For example, if any letter likes "A" in the plain text is encrypted with the any other letter "H" then next time whenever we are going to use the letter "A" in the plaintext, we compensate it with the letter "H" in the cipher text.

F	I	R	S	T
A	M	E	N	D m, e, n, t, a
B	C d, e, f	G	H	K
L m, n	O	P	Q r, s, t	U
V	W	X	Y	Z

Fig 1: Play-Fair by using 5X5 matrix

The Play-Fair algorithm comes under diagraph a substitution cipher which is similar to monoalphabetic substitution cipher. Play-Fair algorithm forms the table by 5 by 5 matrixes with the help of the key that is selected. In Play-Fair algorithm instead of replacing individual letters in the plain text was compensated with a pair of letters.In the Play-Fair algorithm the first step is to split the plaintext into diagraphs and if there is a lone letter, then we must add a null letter to form a diagraph or a pair of letters and this may be usually "X".

The algorithm is Play Fair cipher (or) Wheat stone cipher which is a symmetric encryption algorithmand it is also the first digital substitution cipher. The main propose of algorithm is significantly harder to break by the third person since the frequency analysis is used for simple substitution cipher. Frequency analysis is the analysis of the frequency of letters or group of letters which are used mainly in the cipher text and it is used as assistance for breaking classical ciphers.

4. Proposed Play-Fair Algorithm

In Play –Fair algorithm the key is generated by using 5 by 5 matrixes and the generated key is less secure because as it uses only the alphabet letters in the key generation. But in the modified Play-Fair algorithm by using 9X4 matrixes which contains both alphabets and numbers. The key which is generated by this matrix is more secure as the key contains both alphabets and the numbers. It makes more complicated to the other parties to decrypt the key and to restore the information from the image.

Algorithm for the Proposed Technique

Step 1: Select the message which should be encrypted.

"**Congress shall make law respecting**".

Step 2: The message should be split into pairs

Co ng re sssh al lm ak el aw re specting.

Step 3: Separate all the duplicate letters in the message and by inserting 'X' in between the duplicate letters and continue the new message paring. If same letter repeats more than couple time inserts 'Z' for the third time.

If there is an odd letter at the borderline of the message, just ignore the space and the space should be filled by letter 'X'.

IJSER

Example:

Co ng re sssh al lm ak el aw re specting.

Co ng re sXsZsh al Xl ma ke la wrespect in gX

Step 4: Choose a keyword. The main protocol should be maintained that the keyword should not accommodate with any repeating letters.If any repeating letters are present simply delete the repeating letters.

Key word: "ENCRYPTION"

Step 5: Create a table using the keyword and this table forms 9X4 matrix. For this table to implement, combine the letters I and J in the table.

E	N	C	R
Y	P	T	I
O n	A	B c	D e
F	G	H i=j	K
L	M n, o, p	Q r	S
T	U	V	W
X	Y	Z	1
2	3	4	5
6	7	8	9

Fig 2: Modified Play-Fair table by using 9X4 matrix.

Step 6: By using the table which formed by key word. Now generate the new key by following the simple protocols and this helps in encrypting.

- IF twain letters which appears in the same row, then

Compensate them with the letters to their immediate right respectively.
If the letters are positioned at the borderline of the table, then wrap around.

- IF twain letters appears in the same column, then

Compensate them with the letters to their down one respectively.
If the letters are positioned at the borderline of the table, then wrap around.

- IF twain of them are not in same row and same column and it forms a rectangle, then

If the letters are at two opposite edges then, compensate the letter with the letter that forms at the other edges of the rectangle that which lies in the same row.
If the letters are reaching at the borderline of the table, then wrap around.
Step 7: By using this keyword a new sentence is generated and this sentence is encrypted into the image.

Step 8: Combination of both ambiguous message and image forms a stego image.

Step 9: In decryption the same reverse process is implemented in the reverse manner starting from the stego image.

5. Conclusion

As the rapid growth in the transmission of the databetween the users by using internet as thetransmission medium. It is not only to preserve

IJSER

the data more securely and existence but also the need of privacy should be satisfied. In this paper we approach a modified Play-Fair algorithm by using 9 X 4 matrixes which contains both numbers and alphabets and this mainly helps to encrypt the message more securely into the image and new key is generated and this generated key helps in decrypting the stego image. By using modified algorithm not only the transmission is done over the Stego-image but also the need of privacy is satisfied.

References

[1] T.Morkel, J.H.P.Eloff, and M.S.Oliver, (2005) "An Overview of Image Steganography", in Proc. Of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa.

[2] Stefan Katzenbeiser and Fabien A.P.Petitcolas, (1999) "Information Hiding For Steganography and Digital Watermarking", Computer Security Series, Boston London.

[3] J. Mielikainen, "LSB Matching Revisited", IEEE Signal Processing Letters, vol.13, no.5,may 2006, pp.285-287.

[4] MamtaJuneja and Parvinder Singh Sandhu, (2013) " A New Approach for Information Security Using an Improved Steganography Technique", Journal of Info.Pro.Systems, Vol 9, no:3, pp.405-424.

[5] P.Thiyagarajan, V.Natarajan, G.Aghila, V.PrannaVenkatesan, R.Anitha, (2013) "Pattern Based 3D Image Steganography", 3D Scrutinize center, Kwangwoon University and Springer 2013, 3DR Express., pp.1-8.

[6] Shamim Ahmed Laskar and kattamanchiHemachandran, (2013) "Steganography Based On Random Pixel Selection ForEfficient Data Hiding", International Journal Of Computer Engineering and Technology, Vol.4, Issue2, pp.31-44.

[7] S.ShanmugaPriya, K.Mahesh and DR.K.Kuppusamy (2012) "Efficient Steganography Technique To Implement Selected Least Significant Bits in Spatial Domain", International Journal Of Engineering Scrutinize and Applications,, Vol2, Issue 3, pp.2632-2637.

[8] Hemalatha.S, U.DineshAcharya and Renuka.A (2013) " Comparision of Secure and High Capacity Color Image Steganography Technique in RGB and YCBCR Domains", International Journal Of Advanced Information Technology, Vol.3, No.3, pp.1-9.

[9] Keith L.Haynes, (2011) "Using Image Steganography to Establish Convert Communication Channels", International Journal Of Computer Science and Information Security, Vol 9, No.9, pp.1-7.

[10] Tomas Filler, Student Member, IEEE, Jan Judas and Jessica Fridrich, Member, IEEE, (2010) "Minimizing Additive Distortion in Steganography Using Syndrone Trellis Codes", IEEE Article, pp.1-17.

[11] Jessica Fridich, MiroslavGoljan David Soukal (2006) "Wet Paper Codes With Improved Embedding Efficiency", IEEE Transaction on Information Forensic and Security, Vol 1. No.1, pp 102-110.

[12] M.B.OuldMedeni and El MamounSoudi (2010) "Steganography and Error Correcting Codes", International Journal Of Computer Science and Information Security, Vol.8, No.8, pp147-149.

[13] D.P.Gaikwad and S.J.Wagh, (2010) "Colour Image Restoration for an Effective Steganography", I-manager's Journal on

IJSER

Software Engineering, Vol.4, Np.3, pp.65-
71.

IJSER