Lossless Tagged Visual Cryptography Scheme Using Bit Plane Slicing For Image Processing

Srinivasachar G[1], Shreeram G Hegde [2]
[1]Asst. Professor
[1, 2] Atria Institute of Technology, Visvesvaraya Technological University, Bangalore

Abstract- *Picture steganography is an evolving area of study used for safe information masking and communication over web. The projected scheme gives the path for Least Significant Bit (LSB) based steganography method alongside through Visual Cryptography. Novel information is transformed into encrypted text with the help of undisclosed key then secreted into the LSB of the authentic picture. Using visual cryptography security is increased. Shifting algorithm is used to alter the pixel place of stego image so that the discovery of this message becomes difficult. Visual data is encrypted using visual cryptography. It is achieved with dividing the representation into two shares based on a threshold. The presentation of the projected system is experimented via doing stego investigation, conducting benchmarking test for analyzing the parameters similar to Peak Signal to Noise Ratio (PSNR) and Mean Squared Error (MSE). The major aspire of this proposal is to create the improved safe algorithm which uses both steganography using Visual Cryptography to guarantee superior security and reliability.*

Keywords- LSB, cryptography, stegnography, Visual Cryptography, Stego image, DES

I. INTRODUCTION

Picture steganography, an evolving area of study intended for safe information hiding over networks. The projected scheme gives the way for LSB centred steganography using shifting algorithm. Authentic information is transformed in encrypted text with the use of undisclosed key with a sophisticated ciphering procedure. Later encrypted text is secreted in the LSB of authentic picture via altering the bit array of the novel picture. The resulting picture is called as the stego picture. The stego picture comprises of the data programmed in the LSB of the image. The LSB centred steganography is shared among shifting algorithm to improve safety level of the image. Shifting algorithm modifies the pixel positions of the stego picture thus the secreted information might not be recovered easily. The stego image comprises the secret information that can be easily sent over a wireless network. The intruder, even if he gets access to the image file, would not know that the data is hidden in it. The projected scheme is advanced challenge to RS steganalysis and is a comparison for the regular LSB based steganography method. Steganalysis is the procedure by which picture element of the picture file is analysed to perceive if information is being secreted inside the picture. Steganalysis, the skill as well as science of discovering messages concealed with steganography; this is similar to cryptanalysis useful for cryptography. If it finds any ambiguous distribution of pixels, then it displays the presence of the hidden data showing positive results. By using sShifting algorithm, the chances of detection would be very less due to modification of pixels. Thus, the information is spread all above the picture relatively than at the LSB of the picture. The original image is combined by the secret information to obtain the stego image.

II. LITERATURE SURVEY

LSB method established a visual covert distribution scheme, wherever a picture was broken in n chunks thus merely somebody with every n chunks might decipher the picture, whereas whichever n-1 chunks expose no data regarding the novel picture. Every chunk was written on a distinct transparency and deciphering was done by coating the chunks. While every n chunk is coated, the authentic picture would come into view. With this related thought, transparencies can be adopted to apply a one enciphering, wherever ones clearness is an exchanged arbitrary pad, also other transparency acts as the encrypted text. The representation has been distributed into two shares. Each white pixel in the original picture is split into two of the same small blocks that have full black and white pixels.

When these two blocks are coated, they aligned exactly and so the result is a light-colored block (with half black and half white pixels). Every black pixel in the unique sign is divided in two complementary small blocks. While these two blocks are overlaid, the outcome is a totally black block. Nevertheless each pixel inside the authentic picture is split at arbitrary. In the two shares the same as described over, the shares are connected mutually also reveal the unique image. At rest, while the further share is unidentified, it is hard to differentiate as of a random pattern. Specified merely single share, a next share can be crafted to disclose any possible image; so, individual shares disclose no data regarding the original image.

Information hiding is a method intended for embedding data in cover like picture, aural and filmed records that are used for broadcasting notation, rights safety, honesty verification and secret conversation etc. The majority of information hiding technique inserts messages in the wrap media to create the noticeable media by just modifying the LSB of the wrap making sure awareness simplicity. Thus the implanting procedure will frequently introduce everlasting alteration in the mask. The authentic wrap cannot at all rebuild from the noticeable cover. Yet, in a few adaptations, like medical images, military images and law forensics etc., no deprivation of the authentic wrap is permissible. In this case, there is a unique kind of information thrashing technique is needed, known as reversible data hiding (RDH) or lossless information thrashing, using it the novel wrap is restored without any loss once the implanted information is mined.

A lot of RDH approaches are projected as it was introduced. Fridrich et. Al. [1] offered a worldwide structure for RDH and has embedding procedure separated into three stages. In this the initial phase extracts compressible features without any loss from the unique wrap. In next step compresses the portions with a lossless compression technique which saves room for embedding payloads. Also the ternary phase implants information in the feature sequence and produces the marked mask. One of the reversible implanting techniques compresses the characteristic series as well as adds information next to it forming a customized characteristic series. It restores the novel features to make the noticeable wrap. Hence, later extract information; the recipient can reinstate the novel mask by decompressing the features. Fridrich et. Al. [1] advised features obtained by exploiting distinctiveness of assured picture presentations like texture difficulty and middle-frequency discrete cosine transform (DCT) coefficients for spatial images and for JPEG images accordingly. Tekalp et al. [2] stretched Fridrich et. Al.[1] method by forecasting many LSB planes. And similar idea projected in [1] is casted for reversible information embedding in binary pictures [3], [4] or videos [5]
and [6].

The [7], [8] and [9] techniques have described the different data embedding techniques using LSB approach. The system [7] basically describes the reversible data hiding approach for grayscale images. The MSE and PSNR are most effective in all these systems. Stenography technique was used in [9] for embedding data into image object. The technique projected in [10] and [11] can attain improved routine by applying DE (difference expansion) to forecast errors.

III. SYSTEM DESIGN

The projected form is an addition of the preceding model. The projected scheme makes use of the LSB steganography along with shifting algorithm. The shifting algorithm is used to change the pixel position of the stego picture therefore increasing the safety level to new height. The concealed information is now spread all above the picture relatively than at the LSB of the stego picture. The secret information is initially ciphered using DES (Data Encryption Standard) algorithm. The DES algorithm is used as it is a simple and efficient algorithm uses a little key that can be used for little information. Though the AES (Advanced Encryption Standard), additional superior algorithm that can be used to implant a better system. But, DES is evenly as efficient as AES algorithm. DES is extra complicated encryption algorithm compared to RSA algorithm. The encrypted data is called the cipher information (encrypted data). The cipher information is later encoded to the LSB of the picture and then shifting algorithm is used to change the pixel position of the picture.

Prior to sending the stego picture all the way through the wireless network, the picture is separated into two chunks. The original message can only be retrieved if both the picture shares are obtained. At the recipient side, the two shares are overlaid to obtain the stego picture. Then opposite shifting procedure is applied to acquire the authentic stego representation containing the secret information. The information is cracked from the picture by using suitable decoding algorithm. The information recovered will be in ciphered form and has to be deciphered. The encrypted text is deciphered by the undisclosed (private) key used throughout encryption. The original secret information is recovered at the finale.

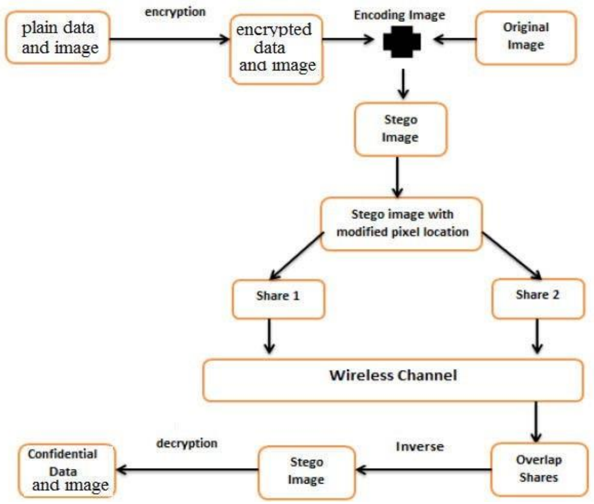

Figure 1 : Proposed System Architecture

Past steganographic methods were not that successful. They used to frequently collapse. So this kind of method will not at all be favored. In these kinds of methods as an alternative of the LSBs a few other bits in the pixel might be altered. Thus this will obviously show a visible dissimilarity. However the projected system produces an output that would look like the original picture as it is. Thus the stego picture would go unobserved while this kind of method is used. Although if the client comes to know that the picture is a stego picture, it is highly not possible to get the novel undisclosed message since the stego picture will merely contain the cipher text.

IV. ALGORITHMS

A. Encryption Phase

In the encryption phase, the original information to be ciphered is provided as input by the user of the software. The text information inserted by the user in the textarea provided is called the original data (confidential data). The encryption algorithm used here is DES.

The DES algorithm is centred on private key encryption. That is the encryption key used is known to the dispatcher and the recipient. Apart from that the encryption key and decryption used are the same. So, the recipient uses the similar encryption key to decrypt at the other end. If the private key is leaked to the receiver then intruder can easily access the information. The result of encryption would be cipher data. Cipher information is worthless information that cannot be understood extremely with any trouble. DES uses a 56-bit key to encrypt the information.

B. Encoding Phase

In this stage, the encrypted information gained is printed into a suitable picture. The data to be encoded is taken from user. After the encode button is pressed, the file chooser opens for selecting suitable picture file for encoding the data. Once picture file selected, it is loaded. It’s better to use .png or .jpg files for programming code information. The picture is initially transformed in a byte symbolism. The byte symbolism is essential to adjust the picture. The encrypted information is transformed into the byte arrangement. The bit-wise procedures are used to add the encrypted information into the picture byte collection bit by bit at the LSB.

C. Pixel Modification Phase

Later the encrypted information has been implanted into the image at the LSB; the picture byte array has to be modified for improving safety and consistency. The LSB approach for information thrashing is not as much secure as might be with no trouble perceived by steganalysis procedure like RS steganalysis. Thus it is superior to change the picture element position wherever the secret data is deposited. The RS study is a well-known steganalysis algorithm having the power to notice the concealed information using arithmetic study of picture elements values. Procedure of RS steganalysis makes use of normal also remarkable group as the consideration in order to estimation the association of pixels. The existence of secret data, strong association have been observed in the neighbouring picture elements. Nevertheless unluckily using old-style LSB replace steganography, the scheme renders the modification in the ratio in remarkable and standard groups which discloses existence of steganography. For picture element change, shifting algorithms are used.

D. Overlapping Phase

The both shares of the similar picture are desired to recover the authentic data. Since the encrypted information is spread in both the pictures, it’s not possible for anybody for obtaining the information by obtaining just a single part of the picture. Therefore both chunks are necessary for getting unique data. Succeeding the shares are obtained, the overlaying (overlapping) stage begins. In overlay stage, one of the chunks is coated above the further one suitably. Once both chunks coated correctly, the unique stego picture can be obtained or else an indistinct picture can be achieved. The information can’t be recovered from an indistinct picture. Thus it’s extremely needed to coat the picture correctly.

E. Decoding Phase

In this stage, code information is cracked from the stego picture. The code information can be regained by the opposite procedure that was engaged by the dispatcher.

F. Decryption Phase

In this stage, the code information is changed in the unique information. The DES algorithm is used in the reverse method using the same enciphering key as used throughout enciphering of the unique information. Lastly, the scheme shows the unique text as well picture.

V. RESULT AND DISCUSSION

The LSB technique is explained with the help of binary values. As exposed in the figure the previous bits of the pixels are replaced through the bits of the code text. Thus the final picture will look like the original picture. The Figure 2 shows the time required for LSB translation and Figure 3 shows the time requisite for number of share making of picture which is done in our experiment 1.

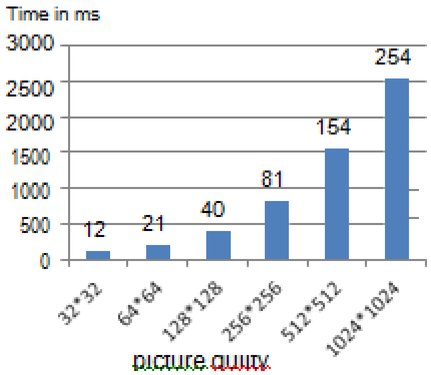

Figure 2 : Time required in milliseconds for LBS conversion

In experiment 2 we have calculated the time for creating the number of shares of specific image. The Figure 3 show the time required for images shares creation.

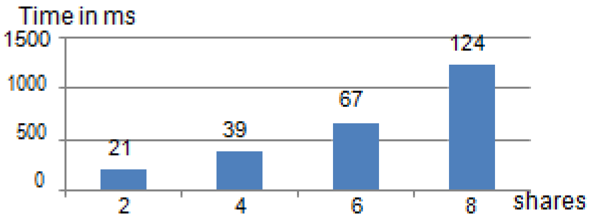

Figure 3 : Time required in milliseconds for image shares creation

In experiment 3 system carried out the performance evaluation with some existing approaches like embedding rate, extraction rate, PSNR and MSE etc. The Figure 4 shows the system comparison with existing system.

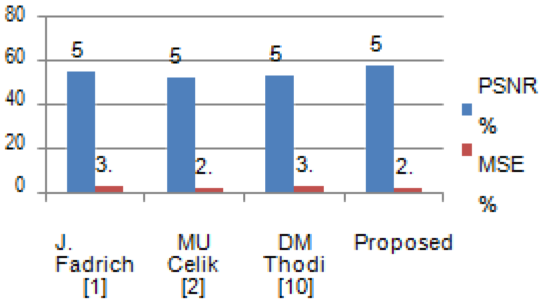

Figure 4 : System performance proposed vs. existing (image size 512*512)

VI. CONCLUSION

The projected scheme securely uses least important bit manipulation based steganography that uses the DES algorithm as well as shifting algorithm all along by visual cryptographic method. It can be completed as usual picture security using steganographic as well

as visual cryptographic method. So the decryption of

the prearranged authentic information becomes a cumbersome try. The safety features of the steganographic methods are extremely optimized using the least significant bit treatment all along with shifting algorithm. The projected scheme gives way to a best grey scale output making it extra resourceful in genuine world application and also can withstand RS assault.

VII. FUTURE WORK

The technique of steganography using visual cryptography in images has its scope in transmission of data in highly secured like trusted as well as untrusted channels. The image data has categorized into unstructured data in big data processing. To implement such approach in big data environment is interesting work for future.

REFERENCES

[1] J. Fridrich, M. Goljan, and R. Du, “Lossless data embedding new paradigm in digital watermarking,” EURASIP Journ. Appl. Sig. Proc., vol. 2002, no. 02, pp. 185–196, Feb 2002..

[2] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, “Lossless generalized- LSB data embedding,” IEEE Trans. Image Process., vol. 14, no. 2, pp. 253– 266, Feb. 2005.

[3] S. Li and A. C. Kot, “Privacy protection of fingerprint database using lossless data hiding,” in Proc. IEEE Int. Conf.Multimedia Expo., 2010, pp. 1293–1298.

[4] Y.-A. Ho, Y.-K. Chan, H.-C. Wu, and Y.-P. Chu, “High-capacity reversible data hiding in binary images using pattern substitution,” Comput. Standards Interfaces, vol. 31, no. 4, pp. 787–794, Jun. 2009.

[5] R. Du and J. Fridrich, “Lossless authentication of MPEG-2 video,” in Proc. IEEE Int. Conf. Image Process., 2002, vol. 2, pp. II-893–II896.

[6] K. Wong, K. Tanaka, K. Takagi, and Y. Nakajima, “Complete video quality-preserving data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 10, pp. 1499–1512, Oct. 2009.

[7] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890– 896, Aug. 2003.

[8] A. M. Alattar, “Reversible watermark using difference expansion of a generalized integer transform,” IEEE Trans. Image Process., vol. 13, no. 8, pp. 1147–1156, Aug. 2004.

[9] H.-J. Kim, V. Sachnev, Y. Q. Shi, J. Nam, and H.-G. Choo, “A novel difference expansion transform for reversible data embedding,” IEEE Trans. Inf. Forensic Security, vol. 3, no. 3, pp. 456–465, Sep. 2008.

[10] D. M. Thodi and J. J. Rodriguez, “Expansion embedding techniques for reversible watermarking,” IEEE Trans. Image Process, vol. 16, no. 3, pp. 721– 730, Mar. 2007.

[11] Y. Hu, H.-K. Lee, and J. Li, “DE-based reversible data hiding with improved overflow location map,” IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 2, pp. 250–260, Feb. 2009.

[12] T. Kalker and F.M.Willems, “Capacity bounds and code constructions for reversible data-hiding,” in Proc. 14th Int. Conf. DSP, 2002, pp. 71–76.

[13] D. Maas, T. Kalker, and F.M.Willems, “A code construction for recursive reversible data-hiding,” in Proc. Multimedia Security Workshop ACM Multimedia, Juan-les-Pins, France, Dec. 6, 2002.

[14] W. Zhang, B. Chen, and N. Yu, “Capacity- approaching codes for reversible data hiding,” in Proc 13th IH, 2011, vol. 6958, LNCS, pp. 255–269, Springer-Verlag