International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

Implementation of Steganographic Algorithms Based on Exact Histogram Matching and Colour Visual Cryptography

Thottempudi Pardhu, R. Sateesh, K. Naveen, K. Mani Raj

Abstract: ***Sensitive secret data transmission through internet has been of great security concern which can be overcome by steganographic methods achieved through secret image sharing. Two novel steganographic secret algorithms based on colour visual cryptography and exact histogram specification is proposed in the present study. The former approach combines colour visual cryptography with a secret key to produce less distorted meaningful share images. A specified histogram acts as the key for the second approach and provides better security and data obscurity compared to conventional approaches. A novel histogram specification method is also proposed which exactly matches the histogram of an image to a specified histogram.***

Keywords: Steganography; Colour visual cryptography; Exact histogram specification; Meaningful Shares

I. INTRODUCTION

Steganography, an ambiguous way of embedding secret data within various seemingly natural media like images, when achieved through shadow image sharing, has various security concerned applications like sensitive data transmission through internet, forensic data hiding, banking applications, biometric authentication, general access structures and digital watermarking. The main requirement of the steganographic methods is to provide high level of security with meaningful shares which are visually normal images.

A steganographic secret sharing scheme called visual cryptography was proposed by Naor and Shamir [1], which basically encrypts a secret binary image into two or more share images which looks like a collection of black and white pixels. Based on the basic idea proposed in [1], many developments have occurred since then, extending the steganographic schemes to grayscale and colour images with meaningful shares. In the present study, two novel secret data sharing schemes, based on colour visual cryptography and exact histogram specification are proposed. The former approach embeds the secret image into two or more meaningful shadow images along with a secret key image. Since the visual cryptography involves random encryption, it always produces meaningful shares with slight artifacts, which can be a matter of suspicion for hackers. The latter approach proposed in the present study aims at embedding the secret message into the histogram of transmitted shares by means of exact histogram specification. Various exact histogram matching techniques are discussed in the literature [2-4]. A straightforward approach for exact histogram specification is proposed in the present study based on which the secret image is embedded.

The paper is organized as follows. Section II explains the various conventional visual cryptography schemes and the proposed steganography scheme based on colour visual cryptography. The novel exact histogram specification algorithm and the data hiding algorithm based on it is explained in section III. The simulation results with analysis and conclusion of the study are particularized in section IV and V respectively.

Revised Manuscript Received on December 30, 2019.

* Correspondence Author

Thottempudi Pardhu*, Assistant Professor, Dept of ECE, MLR Institute of Technology (Hyderabad) India. E-mail: pthottempudi2020@gmail.com

R. Sateesh, Assistant Professor, Dept of ECE, MLR Institute of Technology (Hyderabad) India.

K. Naveen, Assistant Professor, Dept of ECE, MLR Institute of Technology (Hyderabad) India.

K. Mani Raj, Assistant Professor, Dept of ECE, MLR Institute of Technology (Hyderabad) India.

II. STEGANOGRAPHY BASED ON VISUAL CRYPTOGRAPHY

A. Basic Visual Secret Data Sharing Scheme

The basic idea of visual cryptography is to encode a secret image using two or more cover images called shares. The share images are the subset of the original secret image. The semitransparent share images when stacked together reveals the secret image visually, without the need of any cryptographic analysis. The basic procedure can be explained with the help of black and white visual cryptography. If the secret image is a binary image, the task is to encode black or white pixels into two share images. Any one of the share images alone should not reveal any information about the secret image and hence the share images should look like a noisy images consisting of random black and white pixels. A single pixel in the secret image is substituted by two or more pixels in the share images. The encoding table for share generation using four blocks is shown in Fig. 1.

Consider a single pixel replaced by a 2 × 2 block i.e. a 1 or 0 is replaced by different combinations of the set {1,1,0,0}. If the secret pixel is black, the 2 × 2 block in Share-1 will be the complimentary of that in Share-2 because the combination of two shares gives four black pixels where as if the secret pixel is white, the 2 × 2 block in both the shares will be the same so that the combination produces two black and two white pixels, which gives the visual effect of gray colour. The procedure is continued for all the pixels and when the two images are stacked, the black message is seen clearly on a gray background.

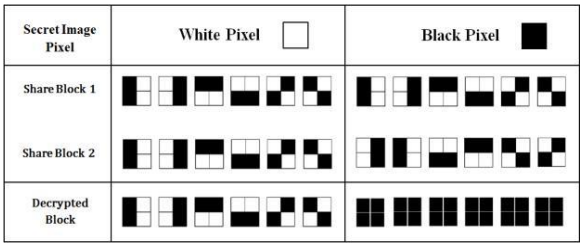

Fig. 1: Basic coding table for visual cryptography

The basic concepts of black and white visual cryptography may be extended to encode colour images using colour shares. Various algorithms for the visual cryptography schemes for colour images with expanded and non-expanded shares are elaborated in [5-8]. The most widely used CVC technique is based on image half toning. The secret image and the cover images are first converted into colour half tone images so that the resultant images contain only eight grey levels; three primary colours, three secondary colours, black and white. The secondary colours can be generated by the combination of primary colours and vice versa. The combination of all the primary colours and secondary colours gives white and black respectively. Hence the eight colours can be represented by three bit combination of ones and zeros. Now the coding logic applied to black and white images can be applied to these half tones images too. A modified CVC scheme which uses four shares along with a key image is elaborated in [8]. An extended CVC scheme which uses error diffusion to reduce the noisy nature of error images is explained in [5**]**.

B. Proposed image steganographic technique based on CVC

In the proposed steganographic technique, the idea of visual cryptography is adopted for embedding the image into shares using random mathematical operation. The CVC encrypted secret image along with a key image may be considered as a computerized steganographic technique because the secret image can be decoded using the computer. Since the images are first converted into halftone and then encryption is applied, the share image seems to be noisy which can grab the attention of a hacker while transmitting them. Using the key image, even though the halftone secret image can be decoded, it is different from the original continuous image. In the proposed method, instead of converting the image into halftone, the different intensity levels of the red, green and blue components of the secret image is divided in a random proportion. A random key block of size 1 × 2 or 2 × 2, with its elements as ones and zeros, is generated.

Corresponding to each pixel in the secret image, an encoded block, in accordance with the key block, is placed in the cover images.

Let S be the secret image which needs to be embedded into N cover images- C_1 to C_N, as share images- SH_1 to SH_N, using a key image K. A secret pixel value S(m,n) is divided in a random proportion $p_1 : p_2 \ldots . : p_N$. Let the decompose values be $S_1(m,n)$, $S_2(m,n)$….., $S_N(m,n)$. A key block K_{mn} corresponding to S(m,n) is generated from {1,1,0,0}. The key block is placed in appropriate positions of the cover images and the ones in each of the share images will be replaced by $S_1(m,n)$, $S_2(m,n)$….., $S_N(m,n)$ and the zeros will be replaced with the original cover image values $C_1(m,n)$, $C_2(m,n)$….., $C_N(m,n)$. Hence the i^{th} share block corresponding to S(m,n) will be a random combination of the set {S_i, $\bar{S}_i$, $C_i(m,n)$, $\bar{C}_i(m,n)$}.

The security can be improved by including different proportions of the secret image within a block in the share image and their positions reversed in the other share image

The procedure is done for all the pixels of the red, blue and green components to generate the share images. For retrieving the secret image, the shares are added together and decrypted using the key image.

III. STEGANOGRAPHY BASED ON EXACT HISTOGRAM SPECIFICATION

A. Exact Histogram Specification

Histogram specification or matching is the set of procedures applied to an image which cause the histogram of the image to match a specified desired histogram or shape. In the classical histogram specification problem, the graylevels of the image are considered as a random variable and the histogram as the probability density function. The statistical approach used in the classical histogram specification problem cannot produce exact matching of the desired histogram. A novel direct histogram matching approach is proposed in the present study based on which data hiding is carried out. The algorithm for exact histogram matching is explained below.

Let contains the specified histogram values. be the image and be the matrix which corresponds to the image with matched histogram which is initialized as

1. Reshape the image of size into a vector of size
2. Sort the intensity values in from lowest to the highest and the corresponding indices are stored in .

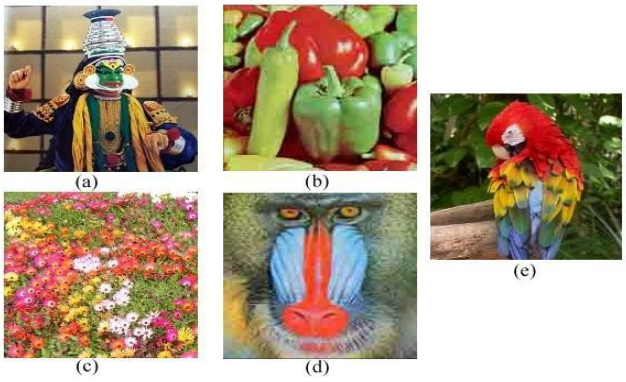

Fig. 2: (a,b,c,d) Cover images (e). Secret Image

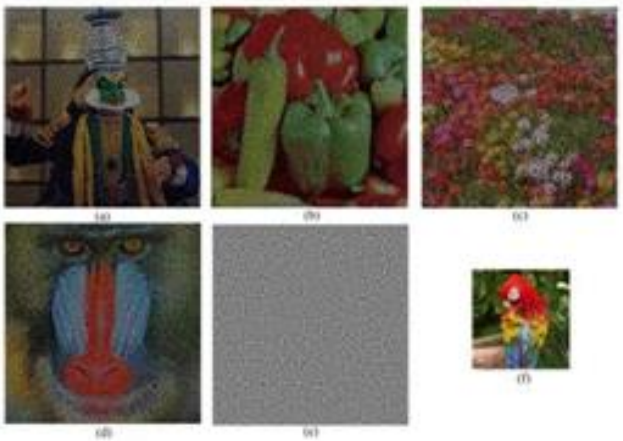

Fig. 3: Conventional CVC method. (a,b,c,d) Share images. (e) Key Image. (f) Decrypted Image.

3. For a particular intensity value, starting from , set variable , select elements from and form a temporary array `
4. From each value in ˆand the total size of the image matrix , find the corresponding row and column co-ordinates, (in the original image matrix.
5. Assign the intensity value to and repeat steps 4 and 5 for all values in ˆ.
6. Increment the intensity value and modify the variable as .
7. Repeat steps 3 to 7 until
8. When , the remaining bright intensity values which will not fit according to the specified distribution are mapped to white. Hence modify ` and repeat the

steps from 4 and 5. is the image with the specified histogram.

B. Proposed data hiding scheme based on exact histogram specification

The problems with the secret data sharing scheme based on visual cryptography is that the share images have a slight noisy nature which gives a hint about a secret image being embedded in the shares. Hence a novel secret sharing scheme is proposed which utilizes the exact histogram specification explained in the previous section. The secret data to be encrypted is converted to binary symbols. The cover images are normalized with respect to histogram, i.e. the histogram of the RGB components of the cover images are matched to a linear or nonlinear expression (or shape) which is known only to the recipient. The decimal value corresponding to bits of the secret image is added or subtracted randomly to the histogram of the normalized images. The selection of depends on the number of bits to be encoded. Now, the cover image histograms are matched with the modified encoded histograms and the images are transmitted. At the receiver, the recipient can decode the original secret message from the difference signal between the secret histogram equation and the received histogram. The images are normalized to ensure that the specified histogram does not degrade but enhances the contrast of the images. The algorithm can be summarized as follows.

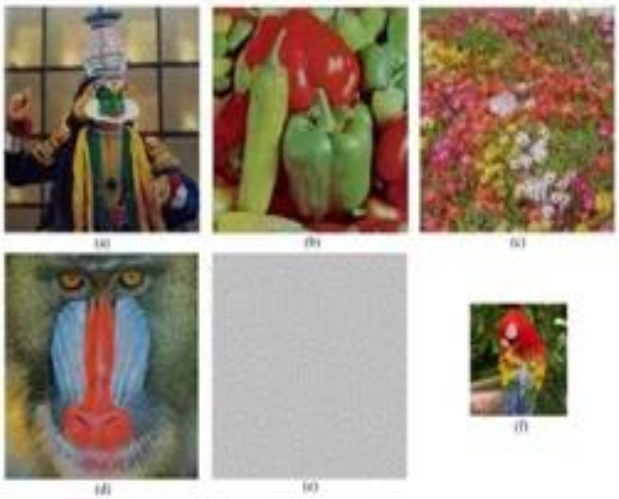

Fig. 4: Proposed method based on CVC. (a,b,c,d) Share images. (e) Key Image. (f) Decrypted Image.

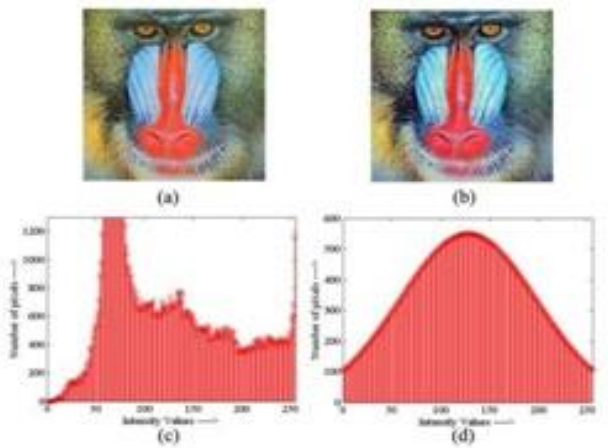

Fig. 5: (a, b) Image before and after histogram specification. (c, d) Histogram of (a) and (b)

1. Generalize the histograms of the RGB components of share images using exact histogram specification

algorithm with the specified histogram, and ensure the visual quality of the image. Convert the secret image (data) to binary and convert each bits to decimal and store in an array,

2. Repeat the array to form an array such that its length is greater than the number of decimal values to be encoded. Randomly add or subtract all elements of with corresponding elements of.
3. Divide the vector into groups of 256 and match the histograms of R, G and B components of the cover images to the divided vectors which gives the encoded share images.

4. For decoding, obtain the absolute error signal between the received histogram and the secret histogram.

5. Convert the error signal to binary and reshape the vector to obtain the secret image (data).

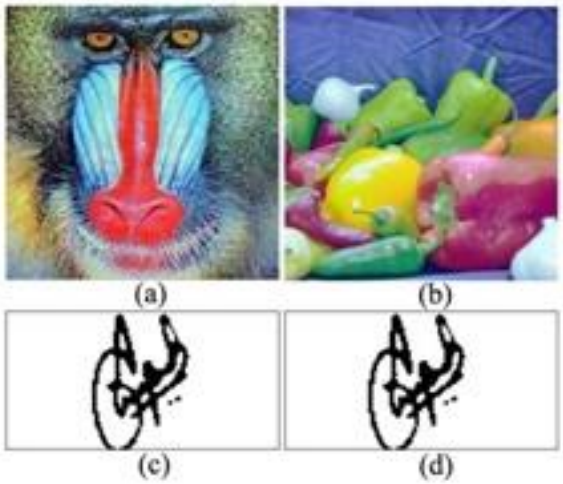

Fig. 6: Proposed method based on Exact Histogram Specification. (a,b) Share images. (c) Secret image. (d). Decrypted image

IV. SIMULATION RESULTS AND ANALYSIS

A. Image steganographic technique based on CVC

Four cover images and secret image of size 177×177 are used in the simulation and are shown by Fig. 2 (a)–(e) respectively.

The share images and the secret key image using the conventional CVC scheme using halftoning technique is illustrated in Fig. 3 from (a)–(e). The secret image from the shares reconstructed is shown in Fig. 3(f). Fig. 4 shows the encrypted share images, key image and the decrypted image using the proposed method. Comparing the share images in Fig. 4 (a)–(d) with that in Fig. 3 (a)-(d), the proposed method produces more meaningful shares with less noise than the conventional shares. The conventional method gives half toned decrypted image, Fig. 3(f) whereas the proposed method produces decrypted image, Fig. 4(f) which is a true colour image, same as the secret image.

B. Steganographic technique based on exact histogram matching

In order to illustrate the effectiveness of the proposed exact histogram specification technique, the histogram of baboon image is matched to obey Gaussian distribution with mean=70 and variance=40, using the proposed technique. The original image and the histogram matched image are shown in Fig. 5 (a) and (b) respectively. Fig. 5

(c) and (d) show the original histogram and the matched histogram of the red component of the image respectively. The secret image to be hidden, which is a scanned signature, is shown in Fig. 6 (c). The encrypted shares and the decrypted image are illustrated in Fig. 6 (a), 6(b) and 6(d) respectively. The shares are not only visually normal images but also have better contrast enhancement and the secret image is exactly recovered from the share images. Since the secret message is embedded into the histogram after exact histogram specification, only the authorized users who know the specified histogram can decrypt the original message which improves the security of the algorithm.

V. CONCLUSION

Two novel secret sharing algorithms are proposed in the present paper and the performance is compared with that of conventional algorithm. For the first algorithm based on CVC, the randomness due to the presence of key image and better quality share images makes it difficult for hackers to decrypt the secret image. The equation for the shape of the specified histogram acts like a key for the second algorithm and it proves to be a better technique for data hiding than the conventional methods. The proposed exact histogram specification procedure may be applied to many other applications like quality improvement and digital watermarking. Data reduction methods may be applied to reduce the size of secret data and the key image produced in the first algorithm may be embedded into one of the share images using the second approach, which may be considered as a future research work.

REFERENCES

1. M. Naor and A. Shamir, “Visual cryptography,” in *Proc. EUROCRYPT*, 1994, pp. 1–12.
2. Sen, D.; Pal, S.K., “Automatic Exact Histogram Specification for Contrast Enhancement and Visual System Based Quantitative Evaluation,” *Image Processing, IEEE Transactions on* , vol.20, no.5, pp.1211,1220, May 2011
3. Seung-Won Jung; Sung-Jea Ko, “Improved exact histogram specification based on the human visual system,” *Selected Topics in Signal Processing, IEEE Journal of* , vol.PP, no.99, pp.1,1, 0, 2011
4. Coltuc, D.; Bolon, P.; Chassery, J.-M., “Exact histogram specification,” *Image Processing, IEEE Transactions on* , vol.15, no.5, pp.1143,1152, May 2006
5. InKoo Kang; Arce, G.R.; Lee, Heung-Kyu, “Color Extended Visual Cryptography Using Error Diffusion,” *Image Processing, IEEE Transactions on* , vol.20, no.1, pp.132,145, Jan. 2011
6. Liu, F.; Wu, C. -K; Lin, X.-J., “Colour visual cryptography schemes,” *Information Security, IET* , vol.2, no.4, pp.151,165, December 2008
7. Yi-Jing Huang; Jun-Dong Chang, “Non-expanded visual cryptography scheme with authentication,” *Next-Generation Electronics (ISNE), 2013 IEEE International Symposium on* , vol., no., pp.165,168, 25-26 Feb. 2013
8. Kamath, M.; Parab, A.; Salyankar, A.; Dholay, S., “Extended visual cryptography for color images using coding tables,”
9. *Communication, Information & Computing Technology (ICCICT), 2012 International Conference on* , vol., no., pp.1,6, 19-20 Oct. 2012

AUTHORS PROFILE

PardhuThottempudi became a Member (M) of IEEE in 2015. Pardhu was born in Luxettipet village in Adilabad district in Telangana state, India. He completed Bachelor’s Degree B.Tech in the stream of Electronics and Communication Engineering in 2011 from MLR Institute of Technology, Hyderabad, India. He has done his Master’s Degree M.Tech in Embedded Systems from Vignan’s University, Vadlamudi in 2013. He is Perusing his Ph.D from VIT University, Vellore,Tamil Nadu His major fields of interests include Digital signal processing, RADAR communications, Embedded systems, implementation of signal processing on applications in FPGA. He is working as Assistant Professor of Department of Electronics and Communication Engineering in MLR Institute of Technology, Hyderabad, India since 2016. He also worked as project intern in Research Centre Imarat, Hyderabad. He published 29 research papers on VLSI, Image Processing, Antennas, Signal processing, RADAR Communications in Reputed International Journals and Various IEEE Conferences. Pardhu Thottempudi is the Life member of ISTE, Associate Member of IETE from 2015. He is the member of IEEE signal Processing society, IEEE Industrial Electronics Society

R.Sateesh is Working as Asst. Professor in Dept of E.C.E , MLRIT, Hyderabad Since 2016. His Research Interests includes, Embedded Systems, VLSI.

K.Naveen is Working as Asst. Professor in Dept of E.C.E, MLRIT, Hyderabad Since 2016. His Research Interests includes, Embedded Systems, VLSI.

K.mani Raj is Working as Asst. Professor in Dept of E.C.E , MLRIT, Hyderabad Since 2014. His Research Interests includes, Embedded Systems, VLSI.