

Secret Data Transfer using Rotation Based Visual Cryptography and LSB based Steganography

Deepa Priya V ¹, Dr. Sundaram M²

Kamaraj College of Engineering and Technology, Virudhunagar, Tamil Nadu, India

ABSTRACT: Visual cryptography is based on cryptography where n images are encoded in a way that only the human visual system can decrypt the hidden message without any cryptographic computations when all shares are stacked together. Steganography is the art of hiding information in other information. After embedding the secret data in the cover image, the cover image remains the same. In this proposed Scheme, the rotation based visual cryptography technique has been implemented for providing security for the secret data. The secret messages can be hiding in the 2 image shares with the use of random degrees of rotation. The secret image shares can be hiding in the cover image by using the technique called pixel value differencing in steganography. The advantage of the proposed scheme is the secret message can be embedded in the two shares of images with help of the rotation operation. High data security can be achieved by using the pixel value differencing algorithms in steganography.

KEYWORDS: Steganography, Visual Cryptography, Pixel value Differencing.

I. INTRODUCTION

Visual cryptography (VC) is the concept of dividing a secret image into 'n' shares and revealing secret image by stacking a qualified subset of 'n' shares. The scheme is perfectly secure and very easy to implement. Visual cryptography takes the input as one secret image and creates the shares (more than one encrypted images) by the process of encryption, later decryption is done by human visual system. Decryption is by done by printing each share on a separate transparency sheet and then placing them on each other. Visual cryptography scheme has many applications like secret sharing scheme, Copyright protection, half toning process and Watermarking. Visual cryptography scheme can also be used for authentication and identification process (visual authentication and identification) this scheme was first introduced by Naor and Shamir [1] in 1994.

The Rotation Visual Cryptography Scheme (RVCS) can be used to encode four secret images into two shares. It demonstrates that four secrets can be recovered clearly by stacking two shares with different angles and the shapes of the reconstructed images do not have distortions by Zhengxin Fu [2] in 2009.

An extended visual cryptography scheme (EVCS) is a kind of VCS which consists of meaningful shares (compared to the random shares of traditional VCS). The construction of EVCS which is realized by embedding random shares into meaningful covering shares by Feng Liu ; Chuankun Wu in 2011

The pixel-value differencing (PVD) [4] scheme provides high imperceptibility to the stego image by selecting two consecutive pixels and designs a quantization range table to determine the payload by the difference value between the consecutive pixels. Besides, it offers the advantage of conveying a large number of payloads, while still maintaining the consistency of an image characteristic after data embedding.

In recent years, several studies have been proposed to improve the PVD method. Wu et al.'s [5] presented a method combining pixel-value differencing and the LSB replacement method. Yang and Weng [6] proposed a multipixel differencing method that uses three difference values in a four-pixel block to determine how many secret bits should be embedded, and Jung et al.'s [7] proposed an image data hiding method based on multipixel differencing and LSB

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015









substitution. Liu and Shih [8] proposed two extensions of the PVD method, the block-based approach and Haar-based approach, and Yang et al. proposed an information hiding technique based on blocked PVD. Liao et al.'s [9] proposed a four-pixel differencing and modified LSB substitution, and Yang et al.'s [10] proposed a data hiding scheme using the pixel-value differencing in multimedia images.

II. VISUAL CRYPTOGRAPHY

The Visual Cryptography technique is mainly used to create n number of shares for the given secret message. There are various schemes available for creating the shares

- **(2,2)-Scheme:** This scheme encrypts the secret image into two shares and obtains the secret image when two shares are superimposed.
- **(2,n)-Scheme:** This scheme encrypts the secret image into n shares and obtains the secret image when two or more of the shares are overlaid. Where „n” represents the number of participants.
- **(n,n)-Scheme:** This scheme encrypts the secret image into n shares and obtains the secret image when all n of the shares are overlaid, but any n - 1 of them will not produce any hint about the secret image. The user has to give the value of n, the number of participants.
- **(k,n)-Scheme:** This scheme encrypts the secret image into n shares and decrypts the secret image when any group of k shares is overlaid, but any k - 1 of them will not give any hint about the secret image. The user has to give the value of k, the threshold, and n, the number of participants.

The Basic (2,2) Visual Cryptography Scheme has been illustrated in the fig 1.

Secret message	Share 1	Share 2	Stacked share
0-bit 			
1-bit 			

fig(1) : Visual Cryptography (2,2) scheme

In this scheme one white or black pixel is expanded into two sub pixels by randomly selecting one of the two ways with the 50% probability as shown in figure1. For black pixel, we get the result in the form of complete black when shares 1 and 2 are combined together, but for white pixel we get the result in the form of gray (it's partially white and black but seems to be like gray color) because 50% of the contrast is lost for white pixel in the encryption process.

III. STEGANOGRAPHY

Steganography is the art of hiding information in information. Steganography has been implemented in two domains spatial and transform. In this proposed scheme, the LSB based spatial domain is used. The secret message can be embedded in the cover image. After embedding, the cover image remains the same i.e., no visual loss of data. In the receiving side, the algorithm is to be used to get the original secret from the cover image.

In the process of embedding a secret message, a cover image is partitioned into non-overlapping blocks of two consecutive pixels. A difference value is calculated from the values of the two pixels in each block. All possible difference values are classified into a number of ranges. The selection of the range intervals is based on the characteristics of human vision's sensitivity to gray value variations from smoothness to contrast. The difference value

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

then is replaced by a new value to embed the value of a sub-stream of the secret message. The number of bits which can be embedded in a pixel pair is decided by the width of the range that the difference value belongs to. The method is designed in such a way that the modification is never out of the range interval. This method provides an easy way to produce a more imperceptible result than those yielded by simple least-significant-bit replacement methods. The embedded secret message can be extracted from the resulting stego-image without referencing the original cover image. Moreover, a pseudo-random mechanism may be used to achieve secrecy protection. Experimental results show the feasibility of the proposed method. Dual statistics attacks were also conducted to collect related data to show the security of the method.

IV. PROPOSED METHOD

A. Embedding

This paper proposes a new scheme in Rotation Visual Cryptography called Rotation Visual Cryptography using basic (2, 2) scheme in which the secret image is encrypted into two shares using the basic (2, 2) visual cryptography scheme with the help of basis matrices concept.

1. First create the secret image share using (2,2) scheme.
2. The Secret image has been divided into two shares.
3. Each share can be divided into block of pixel.
4. Each block can be rotated in random degrees of rotation (90 degree, 180 degree, 270 degree)

Fig 2 shows the flow representation of visual cryptography scheme

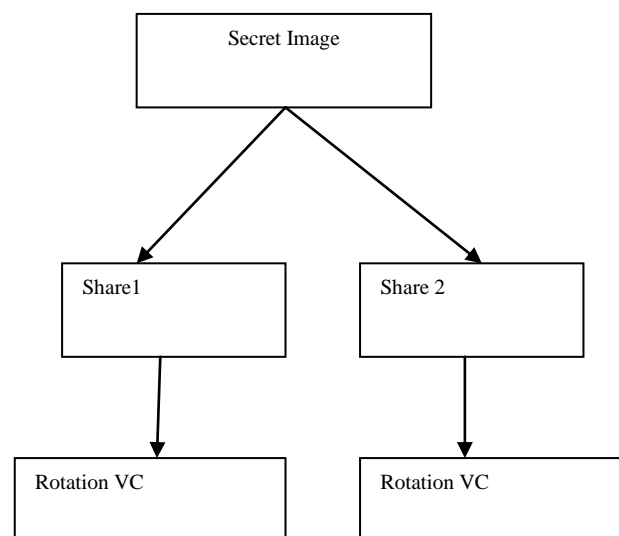


Fig 2: Rotation Visual Cryptography (RVC)

Two Secret shares can be embedded in two gray cover images. The gray images values ranges from 0 to 255. The algorithmic steps for the Secret shares embedding is given below

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

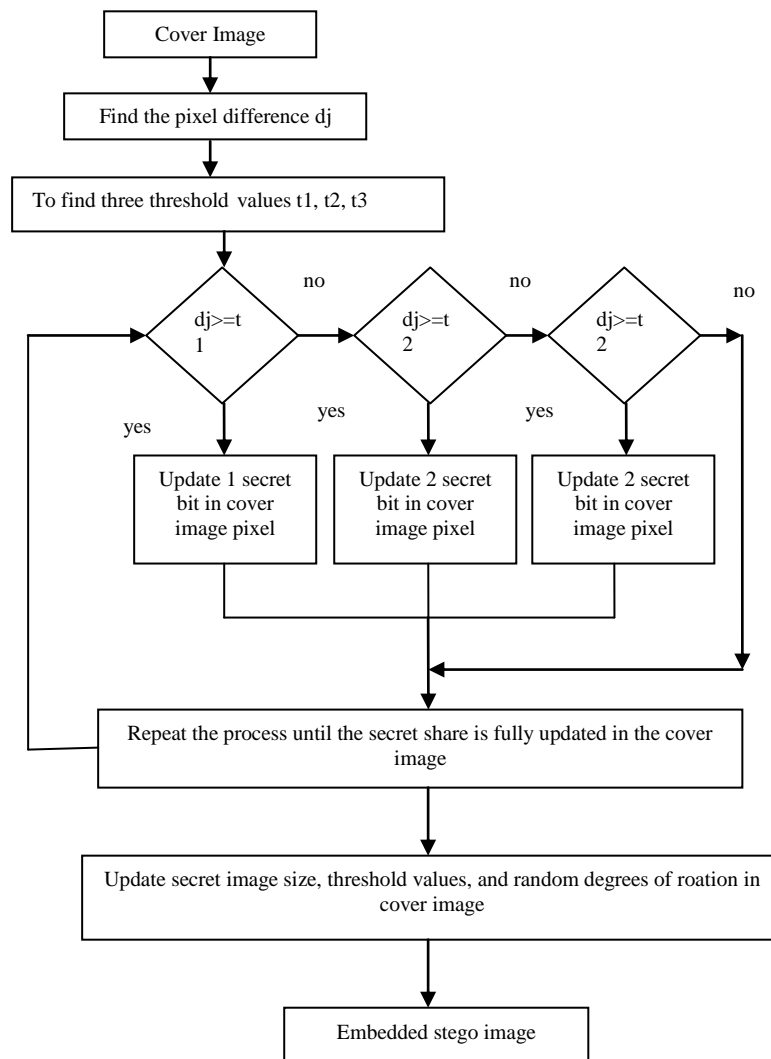


Fig 3: Embedding Shares in cover image

1. The given cover image has been converted into row vector
2. Find the pixel difference between two adjacent pixel $d_j = p_{i+1} - p_i$, Where d_j is row vector
3. Three threshold value T can be calculated by using the formula $T = |p_{i+1} - p_i|$,
4. If the T is in low range then embed only one secret share bit in LSB
5. If the T is in average range then embed two secret share bits in LSB
6. If the T is in high range then embed three secret share bits in LSB
7. If the pixel value greater than 255 after embedding the secret, then adjust the pixel according to the pixel value.
8. After embedding, the row vector of the cover image can be converted into matrix.
9. The cover image remains the same there is no visual distortion in the image.
10. Same procedure is followed for the second secret share.
11. To send the secret share size, threshold and random degrees along with the cover image.

The steps is illustrated in the figure 3

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

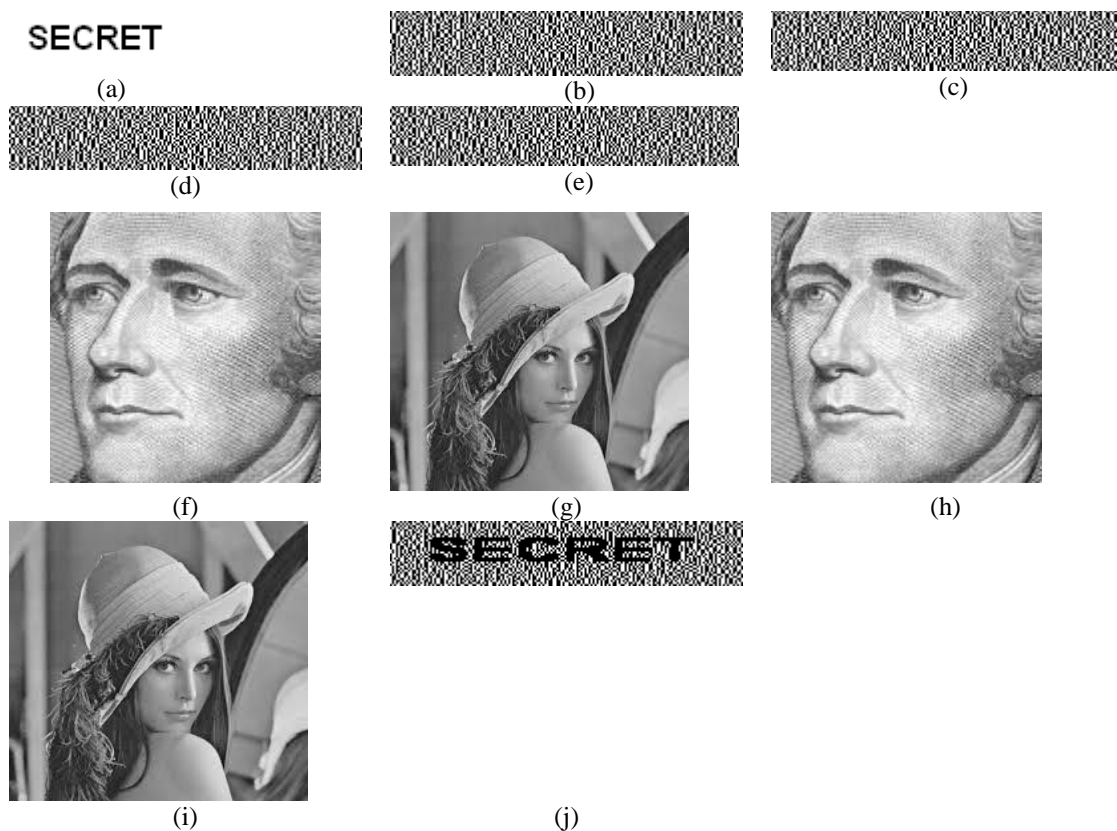
B. Extraction

Once the data is received by the receiver, the receiver extracts the shares from the cover images and applies the random degrees of rotation that can be specified in the embedding procedure. The following algorithm can be used for extracting the secret shares.

1. Convert the given cover image into row vector.
2. To find the Pixel difference between the adjacent pixel $d_j = p_{i+1} - p_i$, Where d_j is row vector
3. If the difference between the pixel values lies in the threshold range T then extract the secret shares from the cover image.
4. If the threshold is very low, then extract one bit from the pixel.
5. If the threshold is average, then extract two bits from the pixel.
6. If the threshold is very high, then extract three bits from the pixel
7. Step 4-6 is repeated to get the complete secret share from the cover image
8. The secret share is divided in to non overlapping blocks and applies random degrees of rotation specified in the embedding stage.
9. Step (1-8) is followed for the second secret share.
10. Stacked share 1 and share 2, to get the original secret message.

V. EXPERIMENTAL RESULTS

Embedding



Figs. 4 Embedding and Extraction shares in cover image (a)Secret Image (b) Secret Share 1 (c) Secret Share 2 (d) Applying rotation in Visual Share 1 (e) Applying rotation in visual share 2 (f) Cover Image 1 (g) Cover Image 2 (h) After embedding share 1 in cover image 1 (i) After Embedding share 2 in cover image. (j) Extracting Secret image by stacking share1 and share 2

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Above Figures shows the results of Embedding and extracting secret shares using rotation visual cryptography and pixel value differencing steganography. Figs. 4(a) shows the secret image. (b) and (c) is obtained by creating the Visual Cryptography (2,2) shares using the secret image. (d) and (e) represents the applying rotation based visual cryptography scheme. (f) and (g) represents original cover images. (h) and (i) represents embedding the secret shares 1 and 2 into the cover image 1 and 2. (j) represents Original secret message extracted from the cover images.

VI. CONCLUSION

The Secure data transfer using rotation based visual cryptography and pixel value differencing image steganography has been implemented. This algorithm successfully embeds and extracts secret data in cover image. The algorithm is applied on many images and found that it successfully embeds and extracts secret data. High data security can be achieved through this algorithm. In future, the same algorithm can be applied for color images and video, audio data.

REFERENCES

- [1] M.Naor and A.Shamir "Visual cryptography", Advances in cryptology EUROCRYPT '94. Lecture notes in Computer Science, (950):1 – 12, 1995.
- [2] Zhengxin Fu "Research on Rotation Visual Cryptography Scheme" Information Engineering and Electronic Commerce, 2009. IEEC '09.
- [3] Feng Liu ; Chuankun Wu "Embedded extended visual cryptography schemes" Information Forensics and Security, IEEE Transactions on Volume:6, Issue:2DOI: 10.1109/TIFS.2011.2116782 Publication Year: 2011 , Page(s): 307 - 322
- [4] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," Pattern Recognition Letters, vol. 24, no. 9-10, pp. 1613–1626, 2003. View at Publisher · View at Google Scholar · View at Scopus
- [5] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Huang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," IEE Proceedings Vision Image and Signal Processing, vol. 152, no. 5, pp. 611–615, 2005. View at Google Scholar
- [6] C. H. Yang and C. Y. Weng, "A steganographic method for digital images by multi-pixel differencing," in Proceedings of International Computer Symposium, pp. 831–836, Taipei, Taiwan, 2006.
- [7] K.-H. Jung, K.-J. Ha, and K.-Y. Yoo, "Image data hiding method based on multi-pixel differencing and LSB substitution methods," in Proceedings of International Conference on Convergence and Hybrid Information Technology (ICHIT '08), pp. 355–358, kor, August 2008. View at Publisher · View at Google Scholar · View at Scopus
- [8] J.-C. Liu and M.-H. Shih, "Generalizations of pixel-value differencing steganography for data hiding in images," Fundamenta Informaticae, vol. 83, no. 3, pp. 319–335, 2008. View at Google Scholar · View at Zentralblatt MATH · View at MathSciNet · View at Scopus
- [9] X. Liao, Q.-Y. Wen, and J. Zhang, "A steganographic method for digital images with four-pixel differencing and modified LSB substitution," Journal of Visual Communication and Image Representation, vol. 22, no. 1, pp. 1–8, 2011. View at Publisher · View at Google Scholar · View at Scopus
- [10] C.-H. Yang, C.-Y. Weng, H.-K. Tso, and S.-J. Wang, "A data hiding scheme using the varieties of pixel-value differencing in multimedia images," Journal of Systems and Software, vol. 84, no. 4, pp. 669–678, 2011. View at Publisher · View at Google Scholar · View at Scopus