An Enhance Scheme of Visual Secret Share for Lossless Recovery

Kalyan Das, Sayantan Samajpati, Abhirup Das, Samir Kumar Bandyopadhyay, Amiya Bhaumik

Abstract*: Algorithms in Visual Cryptography usually uses a sharing scheme where instead of sharing the secret or message directly, it is embedded into multiple shares which are then shared between the intended individuals whereby upon receiving them the decrypting algorithm on the receiving end restores the original secret. A novel cryptographic scheme will not only hide the data, but also will do it in an efficient way which will further ensure that the algorithm is robust to noises and attacks. The proposed algorithm utilizes bitwise operations for efficient hiding of data. Also, it is important that the secret image is losslessly recovered.

Keywords: Key less secret sharing*, lossless *recovery of secret image, Run Length Encoding (RLE).

I. INTRODUCTION

In recent times due to rapid increase in the amount of data shared, it is of prime essence to maintain the security and privacy of that data such that no one other than the intended individual(s) can access the information. [1] Visual cryptography, as coined by Naor and Shamir, breaks the secret message into multiple shares before sharing it. The embedding algorithm ensures that only k or more shares out of n will reveal the secret that is being shared when stacked. Any less than k shares would not be enough.

Visual Cryptography utilizes the human visual system for hiding secret from plain sight. Some of the challenges faced by any Visual Cryptographic algorithm can be summed as a) increased size of the shares, b) distorted or noisy retrieval of the secret, c) requirement of secret channels for sharing keys which are essential for retrieving process etc. Requirement of secret channels involves a third party who generates the keys. By the proposed method all the above-mentioned problems can be avoided.

[2] Marimurugan et al. talked about compressing the secret image before breaking into shares and transmitting them, which would ensure that there is no pixel expansion when embedding the secret in the shares and transmitting them.

Revised Manuscript Received on March 15, 2020.

Kalyan Das, Assistant Professor, Department of Information Technology St. Thomas' College of Engineering and Technology, Kolkata, India

Sayantan Samajpati, Department of Information Technology, St. Thomas' College of Engineering and Technology, Kolkata, India.

Abhirup Das, Department of Information Technology, St. Thomas' College of Engineering and Technology, Kolkata, India.

Prof. Dr. Samir Kumar Bandyopadhyay, Professor, Lincoln University College, Malaysia. Former Registrar, West Bengal University of Technology. Kolkata, India.

Prof. Dr. Amiya Bhaumik, President and Founder Lincoln University College Malaysia.

[3] Shyamalendu et al. proposed an algorithm where the shares generated after embedding the secret reveals the actual secret to some extent and even when less than k (out of n) shares were stacked, though distorted, still revealed the secret image majorly.

[4] Carlo Blundo et al. proposed k out of n shares visual cryptography scheme and although they ensured proper hiding of the secret with less than k (out of n) shares. However, due to optimal pixel expansion the volume to be shared increased.

[5] B.SaiChandana et al. put forward an algorithm which uses a bijective mapping (ie, the function which is used for encryption is reversible which means inverse of that function exists). Although this ensures that the recovery will be lossless but still requires secret key and a resizing factor for proper retrieval of the secret after sharing, therefore requiring secret channel for sharing both the secret key and the resizing factor. The share's volume is same as the secret and hence it's good for limited bandwidth uses. [6] C. C et al. put forward an algorithm which can retrieve the secret image losslessly although it requires sharing of a secret key thereby needing the presence of the secret channel through which the keys will be shared which are needed during decryption and recovering the secret from the shares. [7] Youmaran et al. who put forward the improved algorithm of Chang et al.'s work, also requires a secret channel for sharing the keys for retrieval of the secret image.

[8] Lee et al. talked about embedding meaningless shares, obtained from encrypting the secret image, into meaningful cover images. As a result, the information of the position of each embedded pixel is required for lossless recovery of the secret image. This increases the overall payload of sharing of the secret image as it is not possible to keep the dimensions of both the secret and cover image same without considerable amount of distortions in the retrieved image.

In this proposed algorithm, we can ensure, reduced size of the shares that contains the secret. The algorithm is tested for binary images and the shares compared to the secret are greatly reduced. Unlike some of the above-mentioned B. Sai Chandan et al. this algorithm does not require any secret channel or other form of information for recovering the secret losslessly.

This method also uses Run Length Encoding (RLE) on the secret image for reducing the size of the shares (due to the fact that the secret data to be embedded can be represented in a much lesser space in the shares).

The recovery algorithm is also able to recover the secret from the shares in such a way that there are no distortions in the recovered image.

Also, if 2 shares are generated, all the shares are required for recovery of the secret image, and no less than that of the number of shares generated will reveal anything about the secret that is being shared.

II. PROPOSED METHOD

The proposed method uses the concept of Run Length Encoding (RLE) to compress the pixels of the secret image for reducing the size of the shares. The encoding of the secret image is done in such a way that the white and black pixels are segregated into two shares, one stores the information of the white pixels and the other stores that of the black pixels. This ensures that no single share or any number of shares less than n is enough to reveal any part of the secret image meant to be transmitted. The RLE generates the frequency of a continuous run of black and white pixels which is then encoded in two shares one which holds the white pixel frequencies and the other with the black pixels.

The two shares are used to retrieve the alternate white and black pixel which then recreates the RLE matrix. The RLE matrix is decoded accordingly to reconstruct the original pixels of the secret image, thus resulting in a lossless recovery of the information originally meant to be transmitted between the parties.

The proposed method was tested on a binary image and embedded in random shares. This method requires all the n shares for lossless retrieval of the secret image.

III. MATH

The proposed method uses RLE for generating the frequency of the run lengths of the continuous chunks of black and white pixels. This process can be represented by the following expression:

$$\sum_{i=0}^{n} C(w) + 1\, IF(secret[i][j] == w)$$

$$\sum_{i=0}^{n} C(b) + 1\, IF(secret[i][j] == b)$$

$w \rightarrow white\ pixel$
$b \rightarrow black\ pixel$
$C(w) \rightarrow Count\ of\ contiguous\ black\ pixels$
$C(b) \rightarrow Count\ of\ contiguous\ white\ pixels$

r(w) – stores run length of white pixels
r(b) – stores run length of black pixels
The above can be written in pseudo code as follows:

```
for i in (sizeof(sec))
   for j in (sizeof(sec[i]))
      if sec[i][j] = 0
         r(b) := r(b)  + 1
      if sec[i][j] = 255
         r(w) := r(w) + 1
```

This will give us the row wise run lengths of white and black pixels.
Thereafter these run lengths are segregated depending on the color of the pixels. Now r(w) is stored in s1 share and r(b) is stored in s2 share.

A. Steps for Encryption

Step 1: Generate RLE matrix which contains the frequencies of white and black pixels of each row of the secret image.

Step 2: Embed each value of RLE matrix bitwise into the respective shares i.e., white pixels in one share and black pixels in the other one. This increases the storage capacity of the shares thus reducing the size of the shares to be transmitted. The proposed algorithm uses bitwise replacement since the generated run lengths of the frequencies of the black or white pixels does not always require 8-bits to represent the data. Hence, we can embed multiple run lengths in a single pixel if possible, keeping a specific flag to determine whether a single pixel contain multiple run lengths.

(a) (b) (c)

Fig. 1. Lena image: (a) original, (b) share 1 (embedded with white pixels), and (c) share 2 (embedded with black pixels)

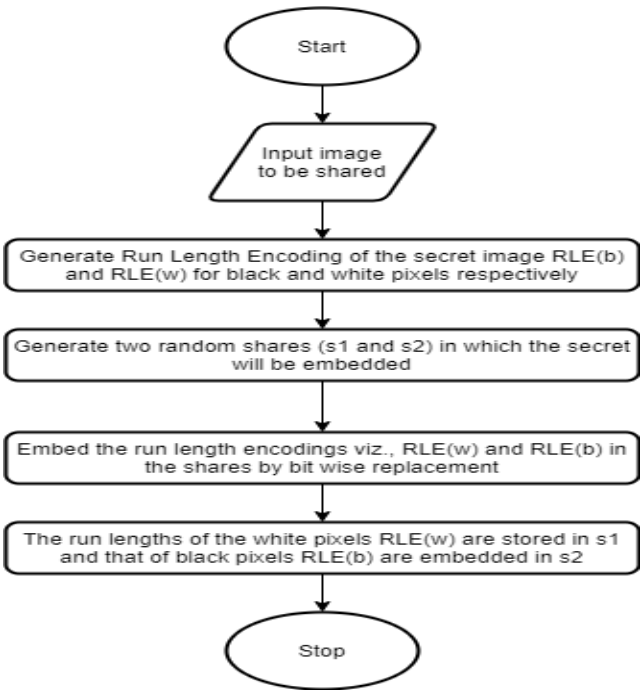
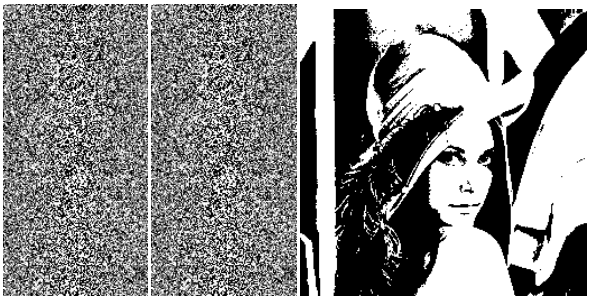


Fig. 2. Flowchart for encryption

B. Steps for Decryption

This proposed method does not require the presence of any secret channel or any form of shared keys. Therefore, the entire secret image can be losslessly recovered or retrieved from just the two shares of the secret image. The steps involving the retrieval of the image are as follows:

Step 1: Retrieve the run lengths of white and black pixels from the respective shares.
Step 2: The retrieved run lengths is used to reconstruct the Run Length Encoding (RLE) matrix.
Step 3: RLE matrix is then decoded accordingly to recreate the information which was originally meant to be transmitted between the parties.



(a) (b) (c)

Fig. 3. Lena image: (a) share 1, (b) share 2, and (c) after retrieval (PSNR = 100 dB)

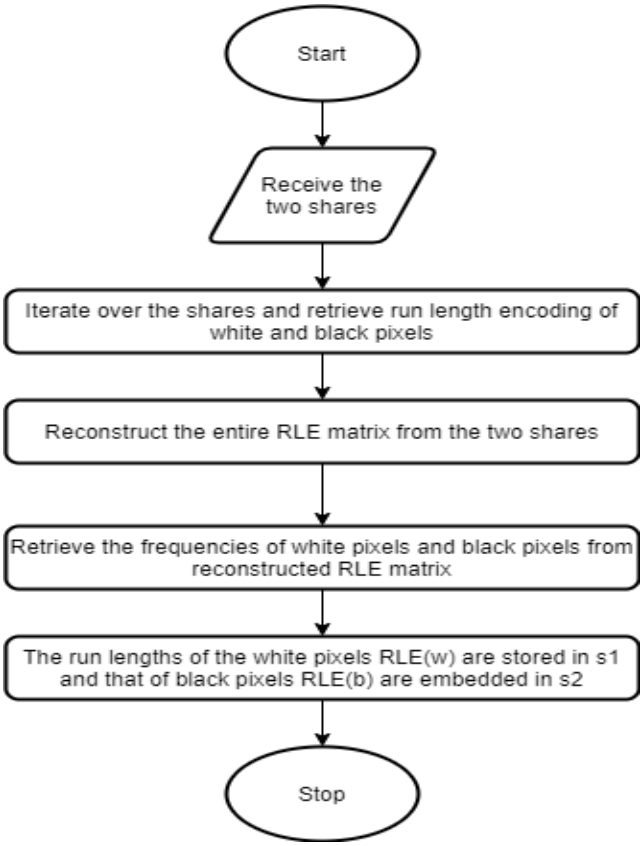
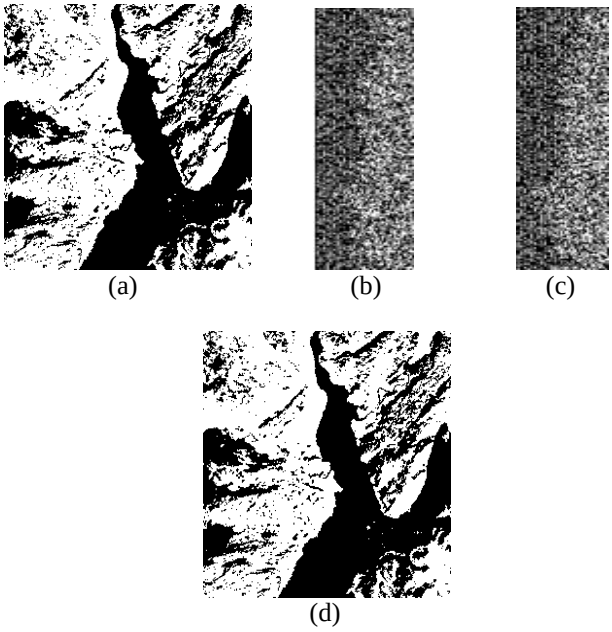


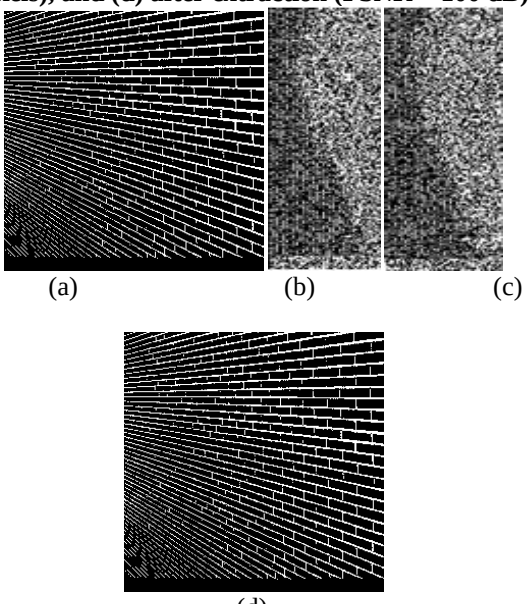
Fig. 4. Flowchart for decryption

IV. RESULT ANALYSIS



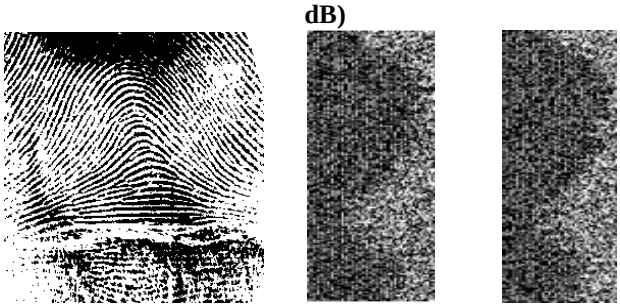
(a) (b) (c) (d)

Fig. 5. Aerial image: (a) original, (b) share 1 (embedded with white pixels), and (c) share 2 (embedded with black pixels), and (d) after extraction (PSNR = 100 dB)



(a) (b) (c) (d)

Fig. 6. Brick wall image (texture): (a) original, (b) share 1 (embedded with white pixels), and (c) share 2 (embedded with black pixels), and (d) after extraction (PSNR = 100 dB)



(a) (b) (c)

(d)

Fig. 7. Fingerprint image: (a) original, (b) share 1 (embedded with white pixels), and (c) share 2 (embedded with black pixels), and (d) after extraction (PSNR = 100 dB)

This proposed method has been applied on various categories of images, including some classic used images, texture images, fingerprint images and some aerial images. The experimental results thus obtained has been shown in the following tables:

Table 1.Experimental Results For Some Classic Used Images

Images (256x256)	PSNR of retrieved image (dB)
Lena	100
Bridge	
Cameraman	
Clown	
Couple	
Crowd	
Girl face	
Man	
Zelda	

Table 2. Experimental results for six texture images

Images (1024x1024)	PSNR of retrieved image (dB)
Carpet	100
Blobs	
Brick wall	
Texture 1	
Texture 2	

Table 3. Experimental results for three fingerprint images

Images	PSNR of retrieved image (dB)
Fingerprint 1	100
Fingerprint 2	
Fingerprint 3	

Table 4.Experimental Results For Eight Aerial Images

Images (256x256)	PSNR of retrieved image (dB)
Aerial 1	100
Aerial 2	
Aerial 3	
Aerial 4	
Aerial 5	
Aerial 6	
Aerial 7	
Aerial 8	

V. CONCLUSION

The proposed method overcomes the following problems associated with the mentioned papers which are as follows:

1. Distortion of the secret image after retrieval.
2. Sharing of keys via secret channel
3. Reduces sizes of the shares of the secret image which are transmitted over the image.

The encryption process since uses bit wise operations which is fast and efficient and therefore can be also used for larger images since its fast from a computer's standpoint. Also it increases the data storing capacity of the shares thereby reducing the size of the shares.

REFERENCES

1. Naor, M., & Shamir, A. (1995). *Visual cryptography. Lecture Notes in Computer Science, 1–12.*
2. Visual Cryptography Based On Modified RLE Compression without Pixel Expansion--Manimurugan.S, Ramajayam.N
3. Shyamalendu kandar et al, "k-n secret sharing visual cryptography scheme for color image using random number," International journal of engineering science and technology vol. 3 no. 3 mar 2011.B. Smith, "An approach to graphs of linear forms (Unpublished work style)," unpublished.
4. Carlo Blundo et al, "Visual Cryptography Schemes with Optimal Pixel Expansion" Universit`a degli Studi di Milano, 26013 Crema, Italy.
5. B.SaiChandana, & S.Anuradha,. (2010). A New Visual Cryptography Scheme for Color Images. International Journal of Engineering Science and Technology. 2.
6. Chang, C. C. and Yu. T. X., Sharing a Secret Gray Image in Multiple Images, in the Proceedings of International Symposium on Cyber Worlds: Theories and Practice, Tokyo, Japan, Nov. 2002, pp.230-237.
7. Youmaran, R., Adler, A., & Miri, A. (n.d.). An Improved Visual Cryptography Scheme for Secret Hiding. 23rd Biennial Symposium on Communications, 2006.
8. Lee, K.-H., & Chiu, P.-L. (2012). An Extended Visual Cryptography Algorithm for General Access Structures. IEEE Transactions on Information Forensics and Security, 7(1), 219–229.

AUTHORS PROFILE

Kalyan Das, Assistant Professor of Information Technology St. Thomas' College of Engineering and Technology, Kolkata, India

Sayantan Samajpati student , Information Technology 4th year. St. Thomas' College of Engineering and Technology, Kolkata, India.

Abhirup Das student , Information Technology 4th year. St. Thomas' College of Engineering and Technology, Kolkata, India.

Prof. Dr. Samir Kumar Bandyopadhyay, Professor, Lincoln University College, Malaysia. Former Registrar, West Bengal University of Technology. Kolkata, India

Prof. Dr. Amiya Bhaumik, President and Founder Lincoln University College Malaysia. He is the Former Vice-Chancellor of Lincoln University College, Malaysia. He is an Executive Vice-President of the International Education Consulting Group, St. Louis, USA since 1999. He was a Research Fellow of UNESCO, Paris. During his tenure, he traveled extensively to Europe, Africa, Asia and Latin America. He served as professor of Business Administration in University of Lucknow, India and in University of Malaya and many other countries.