IJCAT International Journal of Computing and Technology, Volume 1, Issue 4, May 2014
ISSN : 2348 - 6090
www.IJCAT.org

Steganography Combined with RKO Technique for Visual Cryptography

[1] Moushmee Kuri, [2] Dr. Tanuja Sarode

[1] Computer Department, WIEECT , Mumbai University
Worli, Mumbai-Maharashtra, India.

[2] Computer Department, TSEC, Mumbai University
Bandra, Mumbai-Maharashtra, India

Abstract - Numerous algorithms have been proposed in the fields of visual cryptography and steganography with the goals of improving security, reliability, and efficiency. Visual cryptography involves dividing the image into random shares without the use of keys. Since it can be employed by anyone without any cryptographic knowledge and does not require any computations while decrypting, many researches' have been focused on it. Steganography is the art, science, or practice in which messages, images, or files are hidden inside other messages, images, or files. The person sending the hidden data and the person meant to receive the data are the only ones who know about it; but to everyone else, the object containing the hidden data just seems like an everyday normal object. Ultimately they both are ways of hiding data from prying eyes. This paper proposes a method to combine these two strong methodologies of keeping the image and the data secret from the prying eyes. We can develop an algorithm which uses the LSB method of steganography to hide text data inside an image, and then use that image as a secret image for visual cryptography method. The secret image with hidden data will be split up into shares using RKO technique for Visual Cryptography. Then when these shares are re-assembled or decoded to reconstruct the original image the revealed image will still contains the hidden data. The receiver then extracts the hidden data from the revealed image using reverse LSB.

***Keywords*- Steganography, Visual Cryptography, RKO techniquet, Shares, LSB technique.**

1. Introduction

Data is hidden in an image using steganography but the cover image which carries the data can be seen by everyone giving a hint that it carries something. Can we also hide the cover image from the prying eyes? [7].This is exactly where Visual Cryptography plays a role. Hide the data in the cover image using steganography and then create share of this encrypted image using Visual Cryptography. The shares are transferred to the receiver one by one. To extract the data, overlap the received shares and get back the cover image from where the hidden data can be extracted.

As kind of special secret sharing technology, Visual Cryptography (VC) was introduced by Naor and Shamir[1] in the Eurocrypt'94. Since it can be employed by anyone without any cryptographic knowledge and does not require any computations while decrypting, many researches' have been focused on it. This technique does not require any key management nor does it require any algorithm for decryption. A hybrid approach of Visual Cryptography called RKO technique[16] takes the color image and splits the image into two shares. The first share is the random share and the second share is the key share. These two shares have no resemblance to the original image. When the two shares are combined using XOR it reveals the original image. The quality of the image revealed is same as the original image. This algorithm has perfect reconstruction property and there is no loss of picture quality. This algorithm can also be used on gray scale images without any loss of image quality.

2. RKO technique for Visual Cryptography

The RKO technique can be used which splits the image into two shares. The first share is the random share and the second share is the key share. These two shares have no resemblance to the original image. When the two shares are combined using XOR it reveals the original image. The quality of the image revealed is same as the original image. This algorithm has perfect reconstruction property and there is no loss of picture quality. This algorithm can also be used on gray scale images without any loss of image quality[15].

2.1 Algorithm [15]

In step 1: Random Share generation, a random share is generated by taking any random value for R,G and B for each pixel. The size of the share is same as the original image. Every time we create a random share it gives a different value for each pixel. So no two random shares of the same image are same.

In step 2: Key share generation, a key share is generated by xoring every pixel of random share with every pixel of the original image. The size of this share is also same as the original image. No two key shares of the same image are same since no two random shares are same.

In step 3: Overlapping of the shares is done by xoring the random share with the key share pixel by pixel. This results in the generation of the original image.

Algorithm RKO ( )
{
For every pixel i=0 to n
{

$RS_i = R_{(0\text{-}255)} + G_{(0\text{-}255)} + B_{(0\text{-}255)}$

$KS_i = RS_i \oplus OI_i$

}

$OI = RS \oplus KS$
} /* OI = Original Image */

.

3. Image Steganography

Steganography is the art, science, or practice in which messages, images, or files are hidden inside other messages, images, or files. The concept of steganography is not a new one; it dates back many millennia when messages used to be hidden on things of everyday use such as watermarks on letters, carvings on bottom sides of tables, and other objects. The more recent use of this concept emerged with the dawn of the digital world. Experiments have shown that data can be hidden in many ways inside different types of digital files. The main benefit of steganography is that the payload is not expected by the investigators who get to examine the computer data. The person sending the hidden data and the person meant to receive the data are the only ones who know about it; but to everyone else, the object containing the hidden data just seems like an everyday normal object.

3.1 Techniques used for Steganography

There are several different methods and algorithms of hiding data in different types of files. One example of an advanced hiding technique in images is using image layers [13]. This method divides the original image into several blocks, and then creates layers for each block of the binary values of pixels as matrices. The second step to hide the secret bits is to search within these layers' rows and columns and try to find the best match between the binary value of the pixel that is being hidden and the binary value of the pixel where we want to hide it [13]. So for example, if the value of the pixel that we want to hide is '1001', but we did not find a '1001' in any rows or columns of the binary layers of the original image, but we did find a '1000' then this is selected as the closest match and that secret pixel is hidden there.

This method hides less data per block, it only hides 1 byte in an 8 x 8 pixels block whereas other methods like the LSB (Least Significant Bit) matching revisited method hides 1 bit in every pixel [14]. So this method hides less data per block which increases performance and sustains a better image quality. The significant thing about this method is that it doesn't rely on hiding data in the LSB of pixel values, but tries to find the best secret pixel – original image layer pixel binary value match in higher layers of the image thus preserving the quality of the image which makes it somewhat resistant to steganalysis.

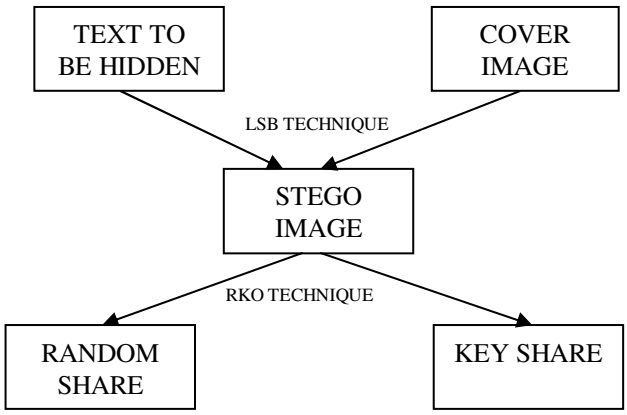
4. Proposed Method

When RKO technique of hybrid Visual Cryptography is combined with Stenography it can be used as an encryption technique used to hide data. The data is first hidden in the cover image. Then using RKO technique the stego image is broken into two shares. The data is now transmitted to the receiver in the form of two shares. At the receiver end the two shares are XORed to reveal the stego image. Then the receiver extracts the hidden text from the stego image by using LSB method.

Since the shares have no resemblance to neither the cover image nor the hidden text it is a perfect technique to hide the data from the intruder as he has no knowledge of what communication is going on between the sender and the receiver. No single share can reveal the text. Both the shares are needed to extract back the hidden text.

The model for this technique is shown in the Figure 1.

SENDER SIDE



RECEIVERS SIDE

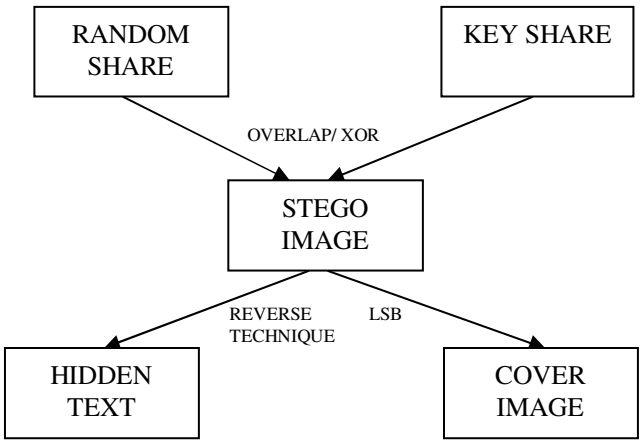


Fig. 1 Model for Steganography combined with RKO technique.

4.1 Encryption

To do encryption, the text to be hidden is specified and the cover image is submitted. The text is hidden in the image using LSB technique of steganography which hides the bits of the message in the LSB bit of every pixel of the image. Since the LSB contains the least information about the image, change in the LSB does not make much change to the image and for the visual eye it appears to be the same image. RKO technique is applied on this stego image and two shares are created. These shares are transmitted to the receiver.

4.2 Decryption

To decrypt the message on the receiver end, the two received shares are overlapped using XOR operator and the stego image is generated. From this stego image the hidden text is extracted and the cover image is recovered as it is.

5. Implementation

5.1 Details

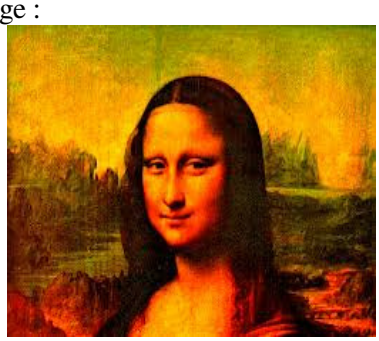
The steganography combined with RKO technique implementation was implemented in JAVA. The encode_text function converts the text to binary and then inserts each bit in the LSB of every pixel.

5.2 Results

Sender Side :

Text : **Visual Cryptography**

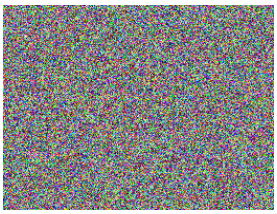
Cover Image :



Stego Image :

Shares Generated :

Random Share

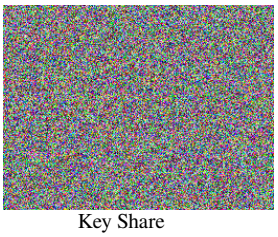


Key Share

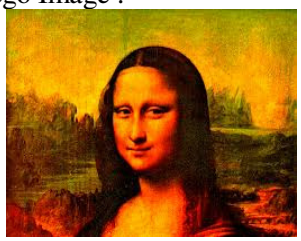
Receiver Side :

Shares Received :


Random Share

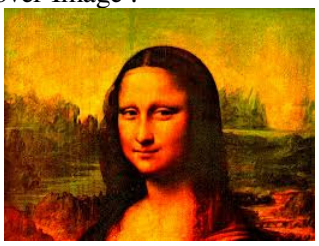

Key Share

Recovered Stego Image :



Recovered Text : **Visual Cryptography**

Recovered Cover Image :



In our proposed scheme the recovered cover image is an exact replica of the cover image as no data is lost during the RKO operations. The extracted text is exactly same as the send text. Hence RKO technique is perfect to be used in conjunction with stegnanography as RKO scheme has perfect reconstruction property. This can be validated using Normalized Correlation (NC). NC is used to measure the correlation between the original secret image and the recovered images from the random shares.

$$NC = \sum_{i=1}^{w} \sum_{j=1}^{h} \frac{\overline{(Sij \oplus Rij)}}{w \times h}$$

S represents the secret image and R the recovered image. w, h represents the width/height of the photographs and $\oplus$ represents the exclusive OR operator. We repeated the test over multiple images, the NC for all the recovered images was 1.000. A comparison of RKO scheme with similar other schemes is listed in Table 1.

Table 1. Comparison of Visual Cryptography Techniques

SCHEMES				
FEATURES	***Kuri, Sarode RKO TECHNIQUE[15]***	***Tsai, Chen et.al. [12]***	***Lukac, and Platanotis [13]***	***Chang and Yu's scheme [14]***
Noise Correlation	Always 1.000	Always < 1.000	1.000	Always < 1.000
Image delivery Transparency	No	Yes	No	Yes
Additional Data Structure	No	Yes AX, BX	No	Yes S-E table (Local)
Key Management	No	Yes S, BX have to be kept secret	No	No
Pixel Expansion (256 color, (n, n) scheme)	No expansion	1 : 9 expansion	1: $2^{(n-1)}$	1 : 529

7. Conclusions

Alone steganography is good method to hide text in images but when steganography and Visual Cryptography are combined together, it is almost impossible for attackers to uncover hidden or encrypted data. The RKO technique used for Visual Cryptography has perfect reconstruction property, the revealed data and the cover image are exact replica of the original. This technique can be used by forensic and security investigators to hide/detect suspicious data. This technique requires less storage as there is no need to store the encryption keys and also requires less amount of computation time as there is no much complex processing. Use of Visual Cryptography makes it impossible for the attacker to even guess that the transmitted shares would contain some hidden data. And even if he somehow gets hold of any one share, it's absolutely impossible to extract data from a single share. So we can conclude that when steganography and Visual Cryptography are combined

together, it is almost impossible for attackers to uncover hidden or encrypted data. And since the RKO technique used, has perfect reconstruction property the recovered image and text are exact replicas of the original.

Acknowledgments

Ms. Moushmee Kuri thanks the guide and TSEC for giving the support and opportunity to carry out the research work in the Visual Cryptography and come up with a new technique called RKO technique and take it to one more level by combining it with Steganography.

References

[1] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT' 94, Berlin, Germany, 1995, vol. 950, pp. 1–12, Springer-Verlag, LNCS

[2] F. Liu1, C.K. Wu X.J. Lin , "Colour Visual Cryptography Schemes", IET Information Security, vol. 2, No. 4, pp 151-165, 2008.

[3] Y. C. Hou, "Visual cryptography for color images," Pattern Recognition, vol. 36, pp. 1619-1629, 2003.

[4] Siddharth Malik, Anjali Sardana, Jaya "A Keyless Approach to Image Encryption", 2012 International Conference on Communication Systems and Network Technologies

[5] L. W. Hawkes, A. Yasinsac and C. Cline, "An Application of Visual Cryptography to Financial Documents," Technical report TR001001,Florida State University, 2000.

[6] George Abboud, Jeffrey Marean, Roman V. Yampolskiy, "Steganography and Visual Cryptography in Computer Forensics", in 2010 Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering

[7] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.

[8] H.-C. Wu, C.-C. Chang, "Sharing Visual Multi-Secrets Using Circle Shares", Comput. Stand. Interfaces 134 (28) ,pp. 123–135, (2005).

[9] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multiple-Image Encryption By Rotating Random Grids", Eighth International Conference on Intelligent Systems Design and Applications, pp. 252-256 , 2008.

[10] Du-Shiau Tsai , Gwoboa Horng , Tzung-Her Chen , Yao-Te Huang , "A Novel Secret Image Sharing Scheme For True-Color Images With Size Constraint", Information Sciences 179 3247–3254 Elsevier, 2009.

[11] R. Lukac, K.N. Plataniotis "Bit-level based secret sharing for image encryption", The Journal of Pattern Recognition Society, 2005.

[12] C.C. Chang, T.-X. Yu," Sharing a secret gray image in multiple images", in: Proceedings of First International Symposium on Cyber orlds, 2002, pp.230–240.

[13] O. Kurtuldu and N. Arica, "A new steganography method using image layers," in Computer and Information Sciences, 2008. ISCIS '08. 23rd International Symposium on, 2008, pp. 1-4.

[14] J. Mielikainen, "LSB matching revisited," Signal Processing Letters, IEEE, vol. 13, pp. 285-287, 2006.

[15] Ms. Moushmee Kuri, Dr. Tanuja Sarode, "RKO Technique for Color Visual Cryptography", in : IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 89-93

Ms. Moushmee Kuri has received B.E.(Computer Engg) dfrom Goa University in 1998, pursuing M. E. Compter Engg from Thadomal Shahani College of Engineering, Bandra, Mumbai, Working as Assistant Professor in Computer Dept. at Watumull Institute of Electronics Engg and Computer Technology., Worli Mumbai. She has more than 10 years of experience in teaching. Has published two papers in the field of Visual Cryptography. Her areas of interest are system Security, system programming and Image Processing.

Dr. Tanuja Sarode has Received Bsc.(Mathematics) from Mumbai University in 1996, Bsc.Tech.(Computer Technology) from Mumbai University in 1999, M.E. (Computer Engineering) from Mumbai University in 2004, Ph.D. from Mukesh Patel School of Technology, Management and Engineering, SVKM's NMIMS University, papers in National /International Vile-Parle (W), Mumbai, INDIA. She has more than 14 years of experience in teaching. Currently working as Associate Professor in Dept. of Computer Engineering at Thadomal Shahani Engineering College, Mumbai. She is life member of IETE, member of International Association of Engineers (IAENG) and International Association of Computer Science and Information Technology (IACSIT), Singapore. Her areas of interest are Image Processing, Signal Processing and Computer Graphics. She has 55 Conferences/journal to her credit.