



iJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 Issue: IV Month of publication: April 2016

DOI:

www.ijraset.com

Call: ☎ 08813907089

E-mail ID: ijraset@gmail.com

Comparative Study of Various Visual Cryptography Techniques to Analyze the Quality of Reconstruction

T. Ambritha¹, J. Poorani Sri², J. Jessintha Jebarani³, M. Pradhiba Selvarani⁴

^{1, 2, 3}UG Student, Department of Computer Science and Engineering

⁴Assistant Professor, Department of Computer Science and Engineering

Kamaraj College of Engineering and Technology, Virudhunagar, TamilNadu.

Abstract: Visual cryptography is one among the cryptographic techniques available, where the secret information is encrypted by giving a key. The secret image will be encrypted into n number of shares. By stacking the shares, the original secret image is decrypted. Here, decryption uses human eyes to recover the secret image without any complex decryption algorithm. Visual cryptography is unique way to protect secrets. This paper compares various algorithms used in visual cryptography in terms of quality, security and size of the recovered image.

Index terms- Secret image sharing, Visual Cryptography, Watermarking.

I. INTRODUCTION

With the growth of internet, more essential data can be accessed through the network. The secure sharing of messages and images is very essential. One possible technique for secure sharing of images and messages is visual cryptography. It is used mainly for security. Cryptography in the study of mathematical techniques related aspects of information security such as entity authentication, confidentiality, and data security [19]. Visual cryptography can be applied for visual authentication and identification any kind images of images like (normal or digital), access control to user images, copy right for images. Visual Cryptography is a new technique that provides information security and uses simple algorithm unlike the complex, computationally intensive algorithms used in other techniques like traditional cryptography [3]. This technique is used to encrypt visual information (pictures, text, etc) in such a way that their decryption can be performed by the human visual system, without any complex cryptographic algorithms. Encryption is a technique used to achieve data security. An encrypted data can be read only if we have access to a secret key or password. This technique encrypts a secret image into shares such that superimposing a sufficient number of shares reveals the original image [12].

II. VISUAL CRYPTOGRAPHIC ALGORITHM

Two main types of encryption algorithms are symmetric encryption algorithm and asymmetric encryption algorithm.

A. Symmetric encryption algorithm

Symmetric Encryption Algorithms can be classified as stream ciphers and block ciphers. Stream ciphers encrypt one bit of image at a time. Block ciphers take a many number of bits and encrypt them as a single unit. Symmetric key algorithm uses same key for both encryption and decryption [7].

- 1) **Data Encryption Standard (DES):** Data encryption standard (DES) is a symmetric algorithm which has got 64-bit block size using a 56-bit key. It gets a 64-bit block of text as input and outputs a 64-bit block of cipher text. It always works on blocks of equal size and also uses both permutations and substitutions. DES has 16 rounds which mean that the main algorithm is repeated 16 times to get the cipher text. In 1999, a network consisting of 10,000 desktops had cracked a DES-enciphered message in less than a day. It was no more invulnerable [7].
- 2) **Triple DES:** Triple DES makes use of a 64-bit key having effective key bits and 8 parity bits. The size of the block is 8 bytes. Triple DES encrypts the data in 8-byte chunks. It is also used to improve the security of DES by applying DES encryption three times by using different keys. It is very secure but very slow [7].
- 3) **Advanced Encryption Standard (AES):** Advanced Encryption Standard (AES) is also a symmetric key encryption technique that is used to replace the Data Encryption Standard (DES). AES uses three key sizes 128, 192 or 256 bit encryption key. The

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

algorithm behaves slightly different with different encryption key size [7]. So the increasing key not only offers a large number of bits but also increase the complexity of the algorithm.

B. Asymmetric Encryption Algorithm

Asymmetric Encryption Algorithm is also known as public key algorithm. It uses different keys for encryption and decryption. Decryption key cannot be obtained from encryption key. The secret message can be communicated securely [10].

- 1) *RSA Encryption Algorithm:* Rivest-Shamir-Adleman (RSA) is commonly used public key encryption algorithm. It is used for encryption and digital signatures. The key size must be greater than 1024 bits for high level of security.
- 2) *Diffie-Hellman:* Diffie-Hellman (DH) is a mostly used key exchange algorithm. If they do not possess any common secret, it could be overcome by a common secret key over an insecure communication channel [10]. When appropriate mathematical group is used, Diffie-Hellman protocol is considered to be secure.
- 3) *Digital Signature Algorithm:* Digital Signature Algorithm (DSA) is not more efficient than RSA for signature verification. The main problem of DSA is the fixed subgroup size as it limits the security to around only 80 bits. Anyway, it is accepted as a good algorithm [20].

III. TECHNIQUES USED

A. Region Incremental Visual Cryptography

Region Incremental Visual Cryptography (RIVC) is a Visual Cryptography Scheme (VCS). It is used for sharing visual secrets in a single image with multiple secrecy levels [5] as shown in Fig 1. In n-level RIVC scheme, an image S is divided into multiply regions associated with n-secret levels encoded to n + 1 share [17]. Some of the features are (a) any of the secrets in S cannot be obtained in any shares. (b) t - 1 level of secrets can be revealed from t ($2 \leq t \leq n+1$). (c) The locations and number of not-yet-revealed secrets are unknown to users. (d) When all the (n+1) shares are available, all secrets in S can be disclosed. (e) Without computation the secrets are recognized by visually inspecting stacked shares [16]. The number of participants engaged in decoding process is proportional to the number of secrets that can be revealed [4].

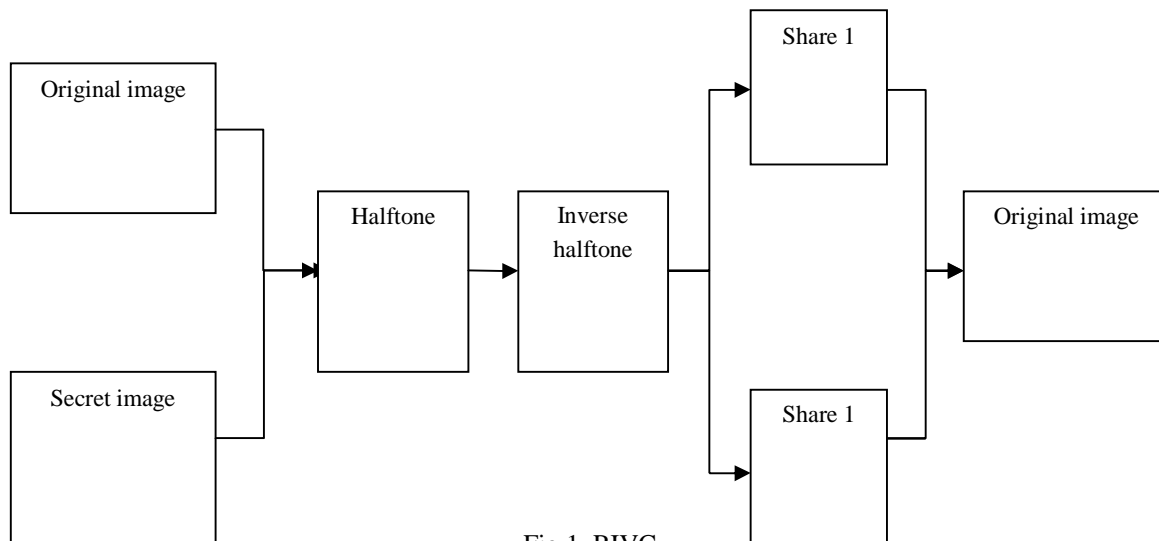
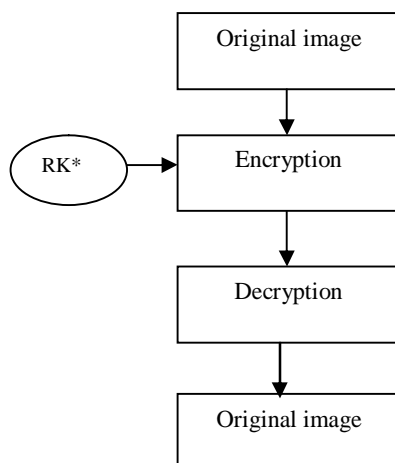


Fig 1. RIVC

B. Visual Cryptography Scheme (with Random Key)

VCS (with random key) can be implemented using Graphical User Interface (GUI) which is a type of interface where users can interact with electronic devices with the help of graphical icons and visual indicators such as secondary notations as opposed to text-based interfaces or text-navigation [15]. The process takes place as shown in the Fig 2. VCS with Random Key generation, consists of many in built functions [9]. GUI operations are very easy to learn and use as it is not needed to be memorized

International Journal for Research in Applied Science & Engineering Technology (IJRASET)



*Random Key

Fig 2. VCS with Random Key

C. (2, 2) Visual Cryptographic Scheme

Visual Cryptography Scheme (VCS) is a method used for protecting image-based secrets and has a computation-free decryption process [1]. In (2, 2) VCS each secret image is divided into two shares in such a way that no information can be obtained from any single share [8]. Transparencies are printed in each shares. Two shares are stacked and secret image can be visualized by human eye without any complex cryptographic computations [14] and this is called decryption as shown in Fig 3. Each pixel P of the secret image is encrypted into a pair of subpixels in each of the two shares [5].

Original pixel	Share 1	Share 2	Share 1 and 2 superimposed

Fig 3. (2, 2)VCS

Some of the disadvantages of (2, 2) visual cryptography scheme are, at first decoding stage, we are unable to get the original image back [18]. Secondly, the cryptographic algorithm becomes more relevant, hence (2, 2) VCS has become inefficient [13].

D. Digital Watermarking

Digital Watermarking is process of hiding a message related to a digital signal (an image, song, video) within the signal itself as shown in Fig. 4. The important property is image fidelity but it alters the original image that leads to degradation of image's quality [6]. The next most important property is effectiveness .The probability that the message in watermarked image will be correctly detected is 1. Here hiding information in images that divide the secret images into multiple shares. It provides more security. The secret information is retrieved by stacking any K number of decrypted shares that reduces color sets and renders the halftone image hence the brightness variation is minimal [6]. Some of the disadvantages of digital watermarking are, when restored

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

watermark pattern from image, selection of pixels is random. When an image has some similarities with the original image, watermark pattern p should restore the image [11].

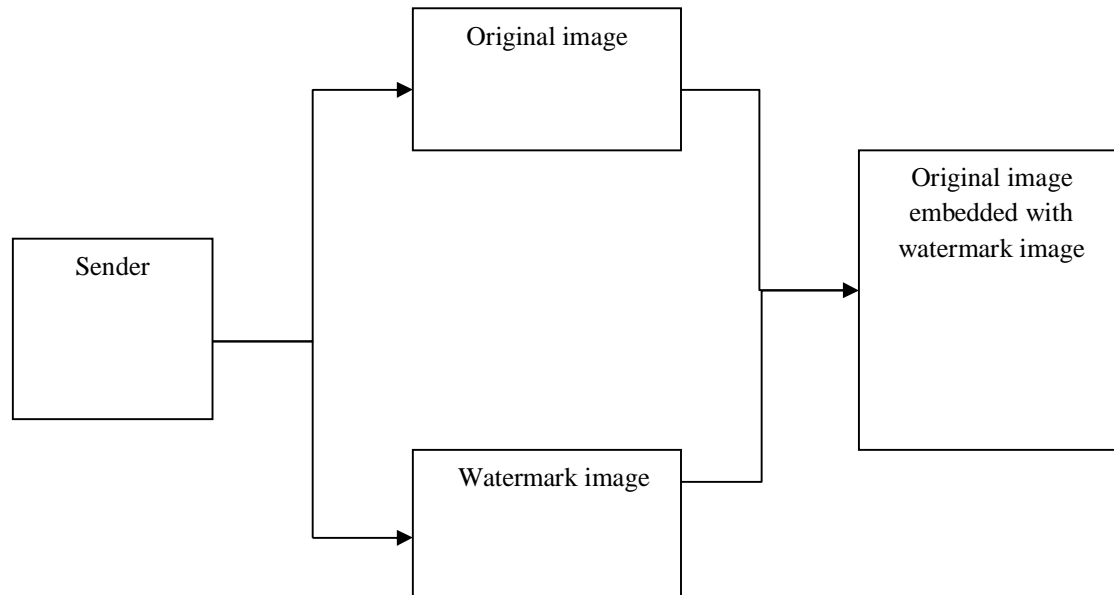


Fig 4. Digital Watermarking

IV. COMPARISON OF EXPERIMENTAL RESULTS

The result of every phase in RIVC is portrayed as in Fig. 5.

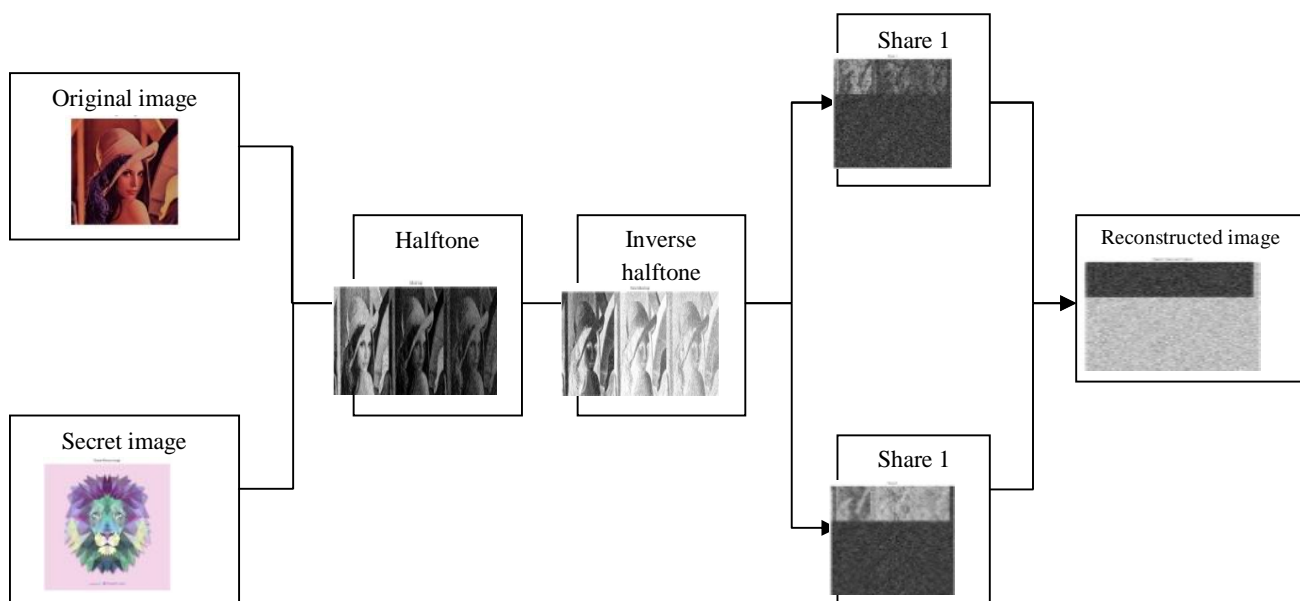


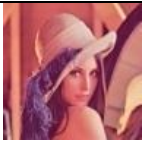



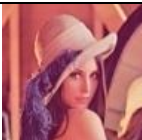
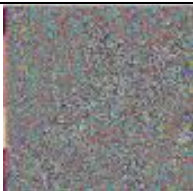
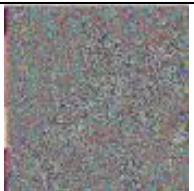

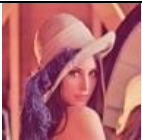
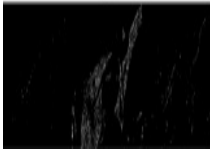
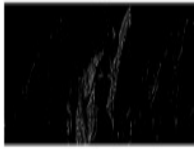

Fig 5. Result of RIVC

The experimental results using various techniques of Visual Cryptography are shown as in the Table 1. The outcomes of VCS with

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Random Key generation and Digital Watermarking were reasonable.

TABLE 1. COMPARISON OF DIGITAL WATERMARKING AND VCS

Techniques	Input Image	Share1	Share2	Output
Digital Watermarking	 Secret image 	-----	-----	 
VCS (with Random Key)				
(2,2)VCS				

The Table 2. shows the comparison of various VCS having the parameters like number of secret images, security level and quality of reconstructed image.

TABLE 2. COMPARATIVE RESULTS OF VCS ALGORITHM

Technique Used	No. of secret images	Security	Result
RIVC	2	Increase	Poor
VCS (with Random Key)	1	Increase	Good
(2,2)VCS	1	Increase	Fair
Digital Watermarking	2	Increase	Fair

V. FUTURE ENHANCEMENT

In the core of VCS, good security level has to be achieved. The recent research works well for text, logos but for color image and gray scale image it works average. The quality of the image was degraded because of halftoning. The future work is to improve the quality, resolution in the obtained reconstructed image and to reduce the noise from it to a greater extent.

VI. CONCLUSION

In this paper, we have done analysis for different visual cryptography schemes and a comparative study has been done. In this

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

technique, the secret image is encrypted into shares such that stacking a sufficient number of shares gives the secret image back. Each and every existing method has its own advantages, yet they have some limitations in reconstructing the input secret image with best quality. Hence, researches are made to figure out a good encryption method.

REFERENCES

- [1] Moni Naor and Adi Shamir, "Visual Cryptography", advances in cryptology Eurocrypt, pp 1-12, 1995.
- [2] Daoshun Wang, Lei Zhang, Ning Ma, Xiaobo Li, "Two secret sharing schemes based on Boolean operations", The journal of the pattern recognition society, 10 November 2006.
- [3] S. Cimato, R. De Prisco, A. De Santis, "Probabilistic visual cryptography schemes", Comput. J. 49 (1) (2006).
- [4] Ran-Zan Wang, "Region incrementing visual cryptography", IEEE Signal Processing Letters Vol. 16, NO. 8, August 2009.
- [5] Nagababu Chekuri, Jhansi Bellampalli, "Region Incremental Visual Cryptography", Bookman International Journal of Electrical & Electronics Engineering, Vol. 1 No. 1 Sep. 2012 ISSN No. 2319-4294© Bookman International Journals.
- [6] Tripta Deendayal, "Enhanced Visual Cryptography Using color Error diffusion and Digital Watermarking", Int.J.Computer Technology & Applications, Vol3 (1), 261-264.
- [7] Jai Singh, Kanak Lata and Javed Ashraf, "Image Encryption & Decryption with Symmetric Key Cryptography using MATLAB", International Journal of Current Engineering and Technology E-ISSN 2277- 4106, P-ISSN 2347- 5161©2015 INPRESSCO International Journal of Current Engineering and Technology, Vol.5, No.1 (Feb 2015).
- [8] Jagdeep Verma, Dr.Vineeta Khemchandani, "A Visual Cryptographic Technique to Secure Image Shares", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 1, Jan-Feb 2012.
- [9] Asha Bhadrar, "An Improved Visual Cryptography Scheme for Color Images", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 02 Issue: 05 | Aug-2015
- [10] Kulvinder Kaur, Vineetha Khemchandani, "Securing Visual Cryptographic Shares Using Public Key Encryption", 3rd IEEE International Advance computing conference, 2013.
- [11] A. Houmansadr and S. Ghaemmaghami, "A novel video watermarking method using visual cryptography", in Proc. IEEE Int. Conf. Eng. Intell. Syst., 2006, pp. 1-5.
- [12] Ching - Nung Yang , Tse - Slih Chen, "Colored Visual Cryptography Scheme based additive color mixing", Pattern Recognition, vol. 41, pp.3114-3129, 2008.
- [13] Young-Chang Hou, "Visual cryptography for color images", Pattern Recognition, 36:1619-1629, August 2002.
- [14] Alkha Mohan, Jayakrishnan A, "Contrast Enhancement in Color Extended Visual Cryptography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 3, March 2015.
- [15] InKoo Kang, Member, IEEE, Gonzalo R. Arce, Fellow, IEEE, and Heung- Kyu Lee, Member, IEEE, "Color Extended Visual Cryptography Using Error Diffusion", IEEE Transactions On Image Processing, Vol. 20, NO. 1, January 2011.
- [16] Ashlin Jose, Divya G, "Region Incrementing Visual Cryptography Using Lazy Wavelet Transform", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 4 Issue 07, July-2015 304.
- [17] J. Tamilarasi, V. Vanitha, T. Renuka, "Improving Image Quality In Extended Visual Cryptography For Halftone Images With No Pixel Expansion", International Journal Of Scientific & Technology Research Volume 3, Issue 4, April 2014.
- [18] Dr. N. Radha, A. Nandhinipreetha, "A Survey on Visual Cryptography Shares", International Journal of Engineering Sciences & Research Technology, ISSN: 2277-9655, March 2015.
- [19] Denslin Barbin, Divya Venkatesan, "Region based visual cryptography scheme for color images", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, No. 3, pp.14731477, 2013.
- [20] Mr. Praveen Chouksey, Mr.Reetesh.Rai, "Secret Sharing based Visual Cryptography Scheme for color preservation using RGB Color Space", IRACST - International Journal of Computer Science and Engineering.

BIBLIOGRAPHY



Ambriitha. T pursuing her UG - B.E (Computer Science and Engineering) degree in Kamaraj College of Engineering and Technology, Virudhunagar, India. She is a Life Member of Indian Society of Technical Education (ISTE). Her area of interest encompasses Visual Cryptography and Network Security.



Poorani Sri. J pursuing her UG - B.E (Computer Science and Engineering) degree in Kamaraj College of Engineering and Technology, Virudhunagar, India. She is a Life Member of Indian Society of Technical Education (ISTE). Her area of interest encompasses Visual Cryptography and Digital Image Processing.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)



Jessintha Jebarani. J pursuing her UG - B.E (Computer Science and Engineering) degree in Kamaraj College of Engineering and Technology, Virudhunagar, India. She is a Life Member of Indian Society of Technical Education (ISTE). Her area of interest encompasses Visual Cryptography and Digital Image Processing.



Pradhiba Selvarani. M received her UG - B.Tech (Information Technology) degree in 2009 from Idhaya Engineering College for Women, Chinnasalem. She then completed her P.G - M.E degree in Computer and Communication Engineering at National Engineering College, Kovilpatti in 2011. She is currently working as an Assistant Professor in Kamaraj College of Engineering and Technology, Virudhunagar, India. She is a Life Member of Indian Society of Technical Education (ISTE). Her area of interest encompasses Pedagogy, Visual Cryptography, Software Engineering and Digital Image Processing.



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)