 ISSN: 2454-4248
06 – 11

Survey on Securing Medical Image Transmission using Visual Cryptography Techniques

[1]I. Diana Judith,
Research Scholar
Department of Computer Science and Engineering
PRIST University, Vallam, Thanjavur,
Tamil Nadu, India

[2]Dr. G. J. Joyce Mary,
Research Supervisor
Department of Computer Science and Engineering
PRIST University, Vallam, Thanjavur
Tamilnadu, India

Abstract: Visual cryptography scheme is a cryptographic technique which allows visual information text or image to be encrypted in such a way that the decryption can be performed by the human visual system and without the aid of computers. It encodes the secret image into shares of different patterns. Visual Cryptography is done on black and white image as well as on color image. This paper includes the literature survey regarding Visual Cryptography techniques for secure medical image transmission.

Keywords: *Cryptography,Visual Cryptography, Halftoning, Secret Sharing Scheme, Error-diffusion,Diffie–Hellman algorithm*

*****

I. INTRODUCTION

In recent days network security has become a main issue. Encryption has come up as a solution, and plays an important role in network security system. Many methods are needed to guard the shared data. Because of the growing demand for information security, image encryption, decryption has become an significant research area and it has broad application prospects.

1.1 Cryptography

Cryptography is a way through which information can be made invisible to the users by encrypting them. It is the study and implementation of techniques to hide information,or simply to protect a message or text from being read.

1.2 Visual Cryptography

Visual cryptography is a powerful encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. Visual Cryptography Schemes (VCS) is a technique of image encryption novel to hide the secret information in images.

Visual cryptography technique was introduced by Naor and Shamir in 1994 as an alternative for conventional cryptography [1]. It uses two or more transient images (called shares). One picture contains arbitrary pixels and the other picture contains the secret information that is hidden. It is not possible to recover the secret information from any one of the pictures (images). Either transparent images or layers are required to reveal the secret information. The simple method to implement visual cryptography is to print the two layers onto a transparent sheet.

When the random imagecontains truly random pixels it can be seen as one-time pad system and will offer unbreakable encryption. In the overlay animation it can be observed by sliding the two layers over each other until they are correctly alignedand the hidden information appears[2]. In visual cryptography, the bit of message consists of a collection of white and black pixels i.e. it is assumed to be a binary image and each pixel is handled separately. Each original pixel appears in n modified versions (called shares) of the image, one for each transparency. Each share contains m black and white sub pixels. Each share of the sub pixels is printed on the transparency in close proximity.

II. LITERATURE REVIEW

Digital image processing is the most potential field in machine vision analysis. Digital image processing refers to processing of two dimensional pictures by a digital computer.In broad spectrum digital image processing can be categorized based on the following image types like Binary Image, Grayscale Image, Color Image and Wavelet based Image. The various image processing techniques like Image enhancement, restoration, segmentation, compression and recognition.

Visual Cryptography (VC) is a special encryption technique to hide the information in an images. It is decrypted by human vision [1]. Various techniques applied in VC which maintains the image quality and security such as Halftone Cryptography, Image Sharing using Steganography, Error Diffusion Technique and Elliptic Curve Cryptography[3]. The major drawbacks in cryptography is hacking of information. In order to avoid the hacking, key generation algorithm is used based by DiffieHellman.The spatial images transfer with high

 ISSN: 2454-4248
06 – 11

security has been mainly contributed the newly proposed system.

Traditional visual cryptography will not send the image with high security. Thus the VCSS comes into existence which is the appropriate approach for transferring highly secured information as text or image.

Halftone Visual Cryptography (HVC) enlarges the area of visual cryptography by the addition of digital Halftoning techniques. In particular, in visual secret sharing schemes, a secret image can be encoded into halftone shares taking meaningful visual information[4]. The secret image is concurrently embedded into binary valued shares while these shares are halftoned by error diffusion, which is the workhorse standard of halftoning algorithms. Error diffusion has low complexity and provides halftone shares with good image quality. A reconstructed secret image, obtained by stacking qualified shares together, does not suffer from cross interference of share images. The main objective of newly proposed system has been performed image sharing with which retains quality of the image. The proposed system using by halftone error diffusion and key generation based in Diffie Hellman algorithm.

2.1 RELATED WORK BASED ON SECURING MEDICAL IMAGES

Security assurance of medical images has dependably been a vital issue in the maintenance of patients' medical records. There is the probability of utilizing visual cryptography for granting protection to medical images[14]. For this situation, a private medical image is dithered into two host images (known as sheets) that are put away in two separate database servers with the end goal that the private image can be uncovered just when both sheets are all the while accessible; in the meantime, the individual sheet images don't uncover the character of the private image. Many authors have assessed the need for security of medical images[17].

2.1.1 Defending the privacy of Patients

Protecting the privacy of every patient's medical records is inevitable and can be done through an encryption scheme. The following works analyzed the need for securing medical images.A sequence of studies on the medical image cryptography affirms the accompanying

1) The probability of concealing a private medical image in two host images.
2) The fruitful coordinating of medical images remade from the sheets.
3) The failure of sheets to uncover the personality of the private medical image.
4) Utilizing distinctive sets of host images to scramble diverse specimens of a similar private image
5) The trouble of cross-database coordinating for deciphering the details of the patients.

The computerized innovation over runs our general public, a limitless number of medical images now exist in database for simple storing, support, and recovery. Pervasive wired and remote systems make it conceivable to get to and share information among medical work force, to advance top notch look after patients[17]. In any case, the accommodation of information gets to and circulation represents an incredible risk on security of patients' data.

2.1.2 Confidentiality of Medical image during transmission

Medical image while transmitting can't be used by unapproved parties (classification) if it is shared as random grid[3], images should not be altered amid transmission (trustworthiness), and images have begun from the right sources to the asserted beneficiaries (confirmation).

Persistently refreshed Digital Imaging and Communication in Medicine (DICOM) models give rules to guarantee confirmation, honesty and privacy of medical images. Safety efforts in DICOM and the examination on Medical image security concentrate on secure stockpiling and secure transmission, before gathering. Be that as it may, after gathering it is feasible for a beneficiary to convey a patient's information to unapproved parties, subsequently abusing the patient's protection.

To the best of our insight, right now nobody has tended to the issue of ensuring patient's protection after the information is got by an approved beneficiary. They mean to fill the hole by concentrate the issue of following unapproved divulgences of medical images. Keeping in mind the end goal to comprehend the multifaceted nature of the issue, we initially need to consider the business show included. To give great medical care, a group of communitarian doctors is frequently framed for a patients' case. These doctors exchange patients' information, for example, images, and analytic reports through open systems.

2.1.3Prerequisite for Sharing Images

The Medicinal faculty can be geologically scattered, and subsequently shape a group correspondence management. Since individuals from the group ought to have the capacity to exchange opinions, one to many(a solitary sender different beneficiaries), or many to numerous (various senders and various beneficiaries) multicast correspondence mode can be received to lessen a sender's calculation and the system data transmission utilization amid gathering correspondence. In such a group correspondence setting, a proficient following plan should be produced to suchan extent that spilled images can be followed back to the encroaching individual source.

The Medical image database of a man are created. It amid treatment and are regularly put away alongside the first crude information. This has uplifted the need of accord security to the subject by enough ensuring the substance of the database. For ensuring the security of an individual medical

 ISSN: 2454-4248
06 – 11

image database. The newly proposed system putting away has been changed medical image format rather than the first layout in the database and it alluded to as a private layout or cancelable medical images.

2.1.4 Security Issues in medical image sharing

Security issues in medical images leads to the novel security system to enhance the security of medical images to protect the patient's privacy. The proposed medical image encryption system in view of confused maps to give security to medical images[5].

The protecting privacy information, for example, content archives and physical signs with patient's medical images for secured storing. The new method was shielded that, the medical records from unlawful access in which the patient as data holder to choose, the authenticated people.

2.1.5 Image encryption and Decryption

Narendra et al. proposed an encryption technique for dark images utilizing a secret key of 128-bits. A histogram moving procedure to reach high piece profundity for secured images was developed.Here the image is conveyed into dynamic pieces and further, these squares are acknowledged through dispersion and substitution strategies[3].

An electronic wellbeing record, which permit sorted out secured images to be joined between endorsed colleagues with a specific end goal to build up the value of medical images [6]. Diffusion based medical image encryption plot was proposed, to show the viability issue, it introduces a substitution apparatus in the stage procedure through somewhat level shuffling strategy. Full security achieved against different assaults for a developed time temporarily. The outcome was exhibited as lossless. Image encryption systems to expand the wellbeing level by introducing creatingshares for images using Anti Phishingusing visual cryptography

2.2 RELATED WORK ON HALFTONE SECRET SHARING SCHEME

Halftoning endeavors to lighten this doubt by having outwardly satisfying characteristics. This implies making halftone shares that convey one snippet of data, for example, another image, while having the secret covered up until both shares are superimposed. This gives no sign that any encryption has been performed on both shares. This in itself definitely enhances the security display for visual cryptography[4].

Novel method by which halftone images can be imparted to critical visual significance which have a higher quality than those exhibited inside by utilizing Error diffusion strategies. These Error diffusion methods spread the pixels as homogeneouslyas conceivable to accomplish the changes in the shares general quality.

Halftone method the shares were enhanced by utilizing contrast upgrade systems. However, the issue with this plan was not impeccably secure. By utilizing a space-filling curve requested dithering strategy, grayscale images can be changed over into an inexact paired image. This permits encryption and decoding of the dim level images utilizing customary visual cryptography techniques[8]. Assist enhancements made around there where accomplished by utilizing better Error diffusion systems, the procedure proposed in fulfills the accompanying 3 necessities:

1) A secret image ought to be a characteristic image
2) Images that convey a secret image ought to be a fantastic regular images
3) Computational cost ought to be low.

This system depends on both (2) and (3) and so as to fulfill (1), brings an extra input instrument into the secret image installing process with a specific end goal to enhance the nature of the outwardly decoded secret image. Strategies depicted in just fulfill some portion of the three prerequisites.

2.2.1 Error Diffusion Halftoning

Franklin et al. portrayed a customary strategy to utilize Error diffusion halftoning procedure which fills in as takes after: two grayscale images are utilized for contribution alongside a secret image. Normally, the secret image can't be utilized as an information image so a ternary image is utilized as contribution to its place. The yield images (that convey the secret) are paired images[13].

First, the image 1 is taken and an Error diffusion process is connected to it (giving offer 1). Then Image 2 has an image concealing Error diffusion prepares connected. Amid this image concealing Error diffusion handle, pixels from image 2 are regulated by comparing pixels of share 1 and the secret image keeping in mind the end goal to implant the secret into the resultant share of image 2. The secret is recuperated by superimposing offer 1 and share 2. The already talked about VC methods all experience the ill effects of pixel development in that the shares are bigger than the first secret image.

2.2.2 Elliptic Curve Algorithm

Visual Cryptographic Biometric Template by methods for the arbitrary stage was proposed. This strategy empowers the encryption of visual information in such a way, to the point that decoding can be done by utilizing the human visual framework. It is found that it has upgraded the security of visual cryptography by scrambling the image by methods for irregular stage.

The new system was developed for cash transfer in view of the Elliptic Curve Discrete Logarithm algorithm. In this technique, the Elliptic Curve Discrete Logarithm was utilized to send the safe encoded message with their open key and gets the scrambled message which is held by their private

 ISSN: 2454-4248
06 – 11

key[12]. Strategy for a Secure E-Cash Transfer on online payment System was proposed.

2.3 RELATED WORK ON ELLIPTIC CURVE DIFFIE HELLMAN ALGORITHM

A productive two-pass elliptic curve Diffie–Hellman key understanding protocol (ECKE-1) that makes utilization of open key verification[19]. This protocol has a place with the class of Diffie–Hellman based key exchange plans bearing Implicit Key Authentication (IKA), i.e. both sides are guaranteed that no different principals beside their proposed work may take in the built up secret key. Strangio guaranteed that protocol ECKE-1 appreciates critical security properties, for example, known-key security, forward secret, obscure key-share flexibility, key control, and key-bargain pantomime strength.

2.3.1 Square based VC

A square based visual cryptography procedure was developed, which utilized elliptic curve to encode and insert the secret image into the cover image. The strategy utilized element obstructing for picking the positions to which the secret image bits are to be implanted. The pixels in HL and LH sub groups of the ECC [3]changed image is chosen for element obstructing since they are identified with solid edges. The strategy is vigorous contrasted with other non-piece based strategies and profoundly reasonable for maps and nearby images.

2.3.2 IntDCT and Diffie Hellman

Another reversible visual cryptography procedure, which depends on Integer Discrete Cosine Transform (IntDCT) and Diffie Hellman (DH) was developed. The image is initially separated into non-covering pieces. The pieces with vitality not as much as some predefined limit is chosen and the distinction development implanting is done on them. This calculation has powerful applications in restorative image handling.

2.4 VC with Elliptic curve Cryptography

ShuFen et al. proposed a visual cryptography strategy which utilizes elliptic curve cryptography. Here, a parallel image is utilized as the secret image. The secret image is then partitioned into two sections, one section is implanted into the first image and the other part is kept by the proprietor. To guarantee proprietorship, the proprietor needs to concentrate one section from the image and recoup with his own particular share.

2.5VC with Diffie Hellman Algorithm

Visual cryptography calculation with Diffie Hellman (DH) was proposed[12]. Here, the secret image is encoded utilizing DH calculation and inserted in the cover image area. The first image is subjected to two levels elliptic curve so as to guarantee power. The secret image is DES scrambled with a key. To decrypt the secret image, the secret key is required.

A new strategy that consolidates encryption and visual cryptography procedures for secure image exchange was developed. This strategy joins visual cryptography, private keys, secret keys and encryption calculations. A secret key is utilized as a part of this technique and is encoded utilizing an asymmetric key algorithm. This secret key is embedded into the encoded image by utilizing visual cryptography calculation[14].

The cryptographic capacities are utilized for encoding the secret image data or to scramble the secret key utilized for visual cryptography. Be that as it may, the determination of installing bits from the first image is very little considered in the above strategies. The cryptographic calculations can be utilized to register values and the secret image can be installed in the first image with the assistance of these qualities, so it will be troublesome for the aggressor to discover where the secret image was implanted.

2.6 VC with Elliptic Curve Diffie Hellman Algorithm(EC-DH)

An encryption conspires with another added substance homomorphism in view of Elliptic Curve Diffie Hellman (EC-DH) for sharing secret images over unsecured channel was developed. The proposed plot empowers shorter key and preferred execution over plans in light of RSA or ElGamal[12]. It has a lower calculation overhead in image decoding contrasting and the technique that utilizations other additively homomorphic property in EC-DH. Elliptic curve parameters are chosen to oppose the Pohlig– Hellman, Pollard's-rho, and Isomorphism assaults. Trial results and investigation demonstrate that the proposed strategy has better execution than RSA and ElGamal.

2.7 VC with EC - ElGamal

Castello et al. connected the added substance homomorphic property of Elliptic Curve EIGamal (EC-ElGamal) in the safe image sharing scheme, and planned a cryptosystem for a productive and generally obvious blend net[9]. The principle motivation behind utilizing the added substance homomorphism of EC-ElGamal is to process the option of the encoded messages and acquire the option of the plaintexts in the wake of decoding. At that point, it can contrast the decoded input respectability evidence and the yield uprightness verification which is the expansion of the yield plaintexts. Along these lines, the e-Voting results are confirmed all around. The visual cryptography framework plan has more concentration on the utilization of properties of Finite Fields[10] and elliptic curves. Added substance and Affine encryption plans utilizing six plans of key groupings

acquired from arbitrary elliptic curve focuses are outlined and explored.

The scrambled images got for this information image and the comparing histograms are examined[6]. It is observed that encoded image does not have lingering data and the comparing histograms are level offering great security for images. The Entropy and the connection coefficient of the info and encoded images are figured and broke down.

The encryption time required for all the eight calculations actualizing every one of these plans are evaluated utilizing a best in class machine while scrambling the cerebrum image. It can be watched that aside from the relative stream figure, different plans can run quick showing their appropriateness continuously applications.

III. CONCLUSION

The survey on encryption for the high quality halftone image has been done with various journals related to the field. The limitations of existing visual cryptography system were also derived from it. The review of literature exposes the actuality that there are various creative visual cryptography approaches. The survey uncovers the fact that despite numerous data on visual cryptography plans has been published, analyzed about with different visual cryptography procedures that consolidate the advantages of different systems in field. This study attempts to propose a visual cryptography scheme for protecting the privacy of images.The future scope of the work is to use 3D Imagesinstead of 2D for creating shares and also improve the contrast of decoded secret image

REFERENCE

[1] M. Naor and A.Shamir. (1995). Visual Cryptography ",Advances in cryptography EUROCRYFT94, LNCS, vol-950, pp.1-12, 1995.

[2] Mahmoud E. Hodeish,V. T. Humbe. (2014). "State-of-the-Art Visual Cryptography Schemes," International Journal of Electronics Communication and Computer Engineering, vol. 5, pp. 412-420.

[3] Srinivasannagara, Raju and Koteswararao. (2015). Image encryption using ECC and Matrix. In proceedings of Intelligent computing, Communication 7 Convergence 2015;48:276-281

[4] G.R Zhi Zhou Arce., G. Di Crescenzo.(2006). "Halftone Visual Cryptography," IEEE Transactions on Image Processing. , Vol. 15, pp. 2441-2453.

[5] R. Vijayaraghavan, S. Sathya, N. R. Raajan. (2014). Security for an Image using Bit-slice Rotation Method–image Encryption. Indian Journal of Science and Technology:April 2014;Vol 7(4S); p 1–7.

[6] M. Naor and A. Shamir. (1994). "Visual cryptography", Proc. Advances in Cryptology (Eurprocrypt'94), pp.1 -12.

[7] C.N. Yang, S.M. Huang. (2010).Constructions and properties of k out of n scalable secret image sharing, Opt. Commun. 283 (9) 1750–1762.

[8] W.-M. Pang, Y. Qu, T.-T. Wong, D. Cohen-Or, P.-A. Heng. (2008). Structure-aware halftoning, ACM Trans. Graph. 27, 89.

[9] C.N. Yang, Y.Y. Chu. (2011). A general (k,n) scalable secret image sharing scheme with the smooth scalability, Journal of Systems & Software 84, 1726–1733.

[10] Chen, Yung-Fu, et al. "A multiple-level visual secret-sharing scheme without image size expansion." *Information Sciences* 177.21 (2007): 4696-4710.

[11] Zhou, Zhi, Gonzalo R. Arce, and Giovanni Di Crescenzo. "Halftone visual cryptography." *IEEE transactions on image processing* 15.8 (2006): 2441-2453.

[12] Myodo, Emi, Hernán Aguirre, and Kiyoshi Tanaka. "Improved image halftoning technique using GAs with concurrent inter-block evaluation." *Genetic and Evolutionary Computation—GECCO 2003*. Springer Berlin/Heidelberg, 2003.

[13] Wang, Zhongmin, Gonzalo R. Arce, and Giovanni Di Crescenzo. "Halftone visual cryptography via error diffusion." *IEEE transactions on information forensics and security* 4.3 (2009): 383-396.

[14] Cimato, Stelvio, and Ching-Nung Yang, eds. *Visual cryptography and secret image sharing*. CRC press, 2011.

[15] Bouslimi D, Coatrieux G, Cozic M, Roux C, A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images, IEEE Transactions on Information Technology in Biomedicine, Volume:16, Issue: 5, Sept. 2012.

[16] Carlo Blundoa, Alfredo De Santis, and MoniNaor, "Visual cryptography for grey level images", Journal of Information Processing Letters Vol.75, pp.255–259, 2000.

[17] Chong, Fu, Wei-hongMeng, Yong-feng Zhan, Zhi-liang Zhu, Francis CM Lau, K. Tse Chi, and Hong-feng Ma. "An efficient and secure medical image protection scheme based on chaotic maps." *Computers in biology and medicine* 43, no. 8 (2013): 1000-1010.

[18] Gil Jae Yu, Eun-Joon Yoon, Sang-Ho Shin and Kee-Young Yoo. A New Image Steganography Based on 2k Correction and Edge-Detection. ITNG Proceedings of the Fifth International Conference on Information Technology: New Generations Pages 563-568, 2008.

[19] Nitty Sarah, Alex, and L. JaniAnbarasi. "Enhanced image secret sharing viaerror diffusion in halftone visual cryptography." In Electronics Computer Technology(ICECT), 2011 3rd International Conference on, vol. 2, pp. 393-397. IEEE, 2011.

AUTHOR'S PROFILE

I.Diana Judith received M.E degree in Computer Science and Engineering from the Department of Computer Science and Engineering in PeriyarManiammai University, Thanjavur, Tamilnadu, India. She is a Research Scholar in the Department of Computer Science and Engineering, Center for Research and Development, PRIST University, Vallam, Thanjavur, Tamilnadu, India. She is working as Assistant Professor in the

 ISSN: 2454-4248
06 – 11

Department of Computer Science, Stella Maris College, Chennai. Her area of interest includes Visual Cryptography, image encryption and decryption.

Dr.G.J.Joyce Mary completed her Ph.D in the area of Parallel Computing in 2012. She is a Research supervisor in the Department of Computer Science and Engineering, PRIST University, Thanjavur, Tamilnadu, India. Her area of interest includes Parallel Computing, Digital Image Processing, Visual Cryptography andWebservice.