IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

A Survey on Visual Cryptography Techniques used in Medical Images Encryption

C. Punithadevi[1*], G. Shanmugasundaram[2], B. Thenmozhi[3*], G. Raga[4], Kreethika Jain[5]

[1,2,3,4,5]Dept. of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry, India

[*]*Corresponding Author: punithadevi@smvec.ac.in Tel.:+91-94423 00345*

DOI: https://doi.org/10.26438/ijcse/v7i3.363370 | Available online at: www.ijcseonline.org

Accepted: 23/Mar/2019, Published: 31/Mar/2019

Abstract— Medical pictures and patient's data are exchanged between various teams to be investigated and assessed by experts who are topographically separated. Any illicit alteration in this data or the event of information loss during the transmission over an uncertain channel may prompt wrong presumptions which may cause an unfavorable impact on patients. Hence, the security of medical images is always been a concern. This security can be provided by the concepts of cryptography. When it is the case of images, an effective security can be provided by using various methods in the domain of Visual Cryptography. In this paper, the various methods used in encrypting the medical images, their efficiency and drawbacks are discussed. A relative analysis based on the performance metrics utilized in these procedures is provided. This article also explores the various key factors and challenges faced in Visual cryptography techniques.

Keywords— Medical images Encryption, Visual Cryptography, Visual Cryptography Techniques, Medical data security

I. INTRODUCTION

Cryptography is the process of protecting information by transforming it into a secure format. So that, only the authorized and authenticated communicating parties can read and process the information. It is the art of hiding text and numbers using certain codes and algorithms. Visual cryptography [1] is a cryptographic technique which is a secret sharing method where the encoding of the input image into 'n' number of shares is done. Its definite procedure is to partition a secret image into irregular shares which independently uncovers no information about the secret image other than its length. In this scheme [2], the secret image can be recovered without any cryptographic learning and computational equipment.

Halftoning is said to be the key process in visual cryptography. Initially, the input image will get separated into two or more shares (n shares) according to the technique or method used. These shares are then processed and transmitted. The communicating party on the other side will receive only the shares, which are then combined in a particular order to recover the actual image.

The benefits of visual cryptography [3] are simple to implement, no need of decryption algorithm, cipher text can be sent through FAX or E-MAIL and secret message can be recognized only by human eyes, so computational cost is low.

The various applications [4] of Visual Cryptography are,

- Biometric Security
- Printing and Scanning applications
- Bank Customer Identification
- Cyber Crime
- Health sector

The field of Medicine involves exchanging medical images and patient's information from one place to another through different forms of electronic telecommunications. Applications [5] related to telecommunications are: Tele-consulting, Tele-radiology, Tele-diagnosis, Tele-surgery, remote medical education, etc. These applications are associated with various types of risks like loss of data during the sharing of medical information across the vulnerable public networks. There exists an opportunity for wrong releases from associations that originate from either approved clients, who purposefully alters the data by violating the authoritative policies or intruders who break into an association's computer system. This results in invading a patient's privacy or prescribing inappropriate medication to the patients which leads to severe consequences. These issues are solved by various techniques using Visual Cryptography.

The efficiency of a technique can be determined by using certain parameters [6] such as input image type, number of shares the original information is got split into, the type of

the share, quality of retrieved secret image etc. The quality of retrieved secret image is calculated by using the values of PSNR (Peak Signal to Noise Ratio), WSNR (Weighted Signal to Noise Ratio), LDM (Linear Distortion measure), UQI (Universal quality index) and MSE (Mean Square Error).

II. VISUAL CRYPTOGRAPHY- KEY FACTORS

In this section, the various key factors and parameters that are considered to evaluate the efficiency of the techniques and the quality of image are discussed.

.

a. Input Image

The input image [7] can be of two types such as Grayscale and Colored images

1) *Grayscale Images*: Grayscale image contains only the shades of grey. The grayscale image is stored as one byte integer that gives 256 likely distinctive shades of grey from black to white.
2) *Coloured Images:* It is necessary to provide three samples for each pixel in coloured images, which are interpreted as coordinates in some colour space. These samples are considered to measure the intensity and chrominance of light.

In grayscale images, less information is enough to represent each pixel when compared to coloured images. For efficient processing, the coloured images can be converted into grayscale images and then processed. Thus, the grayscale images are mostly preferred in Visual Cryptography.

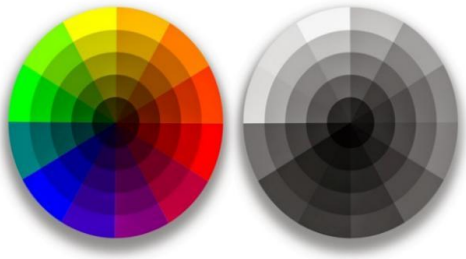

Figure.1. The comparison of color image and grayscale image

b. Share Type

The share type [7] can be of two types such as meaningful share and noise-like share.

i. Meaningful share: The share on which some meaningful cover image is imposed, is said to be a meaningful share.

2) Noise-like share: The noise-like shares are the shares having irregular salt-pepper noise on cover of shares.

c. PSNR

Peak Signal-to-Noise Ratio (PSNR) [7] is an error metric used to compare image compression quality. It represents a measure of the peak error.

The term PSNR is characterized as the proportion between the most extreme possible value of a signal and the power of distorting noise that influences the quality of its representation. Since numerous signals have a wide and dynamic range, in which the proportion between the biggest and smallest possible values of an alterable amount... The PSNR is communicated as far as the logarithmic decibel scale. The higher the PSNR value, higher the image quality.

$$PSNR = 10.\log_{10}(255^2 / MSE)\ (dB)$$

d. WSNR

Weighted Signal-to-Noise Ratio (WSNR) [9] is determined in the spatial frequency area. Human Visual System is a nonlinear, spatially varying system. SNR is an energy-dependent measure. In the time or spatial domain, all samples have the same "weight" (uniform weighting). The higher the WSNR, the better the image quality.

e. LDM

Distortion means any adjustment in the state of a signal's waveform. When a small change occur in the shape of a sine wave, or any signal, the distortion is created.

The term 'linear distortion' is defined as any modification to the signal that will not change the state of the individual sine wave components of a signal. This happens because of the inconsistency in the frequency response, or it could mean a change in the relative stage (timing) of the different frequencies. It can fluctuate the measure of the individual sine wave components, or shift them in time, but it will not bend them. The computation of this linear distortion is called as the Linear Distortion Measurement (LDM) [7]. The lower the LDM, the better the image quality.

f. MSE

Mean Square Error [7] is characterized as the total squared error between the compressed and the original image. It is the estimation of quality of recovered image to the original image. It figures a positive value from 0 to 1; values close to 0 represent better visual quality of image.

$$MSE = 1/MN \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - R(i,j)]^2$$

g. UQI

Universal Image Quality Index (UQI) [10] is the comparison between original and distorted image into three comparison: luminance, contract and structural comparison. The higher the UQI, the better the image quality.

Thus, the parameters required to estimate the image quality and the essential key factors of the visual cryptography techniques are discussed.

III. RELATED WORKS

In this section, various techniques and methods used in Visual Cryptography and its challenges are discussed.

A. Randomised Visual Secret Sharing Encryption

Nikhil C. Mhala et al.., [7] proposed that the better visual quality of reconstructed image was achieved by using the technique called Randomized Visual Secret Sharing Encryption. Here block based progressive visual secret sharing and Discrete Cosine Transform (DCT) based reversible information embedding technique was utilized to recover the secret image. But it failed to generate shares of color images and the difficulty of pixel expansion was not resolved.

B. Error Diffusion Method

To obtain better quality halftone image Kirti Rawat [8] used advanced halftone scheme using matrix Error Diffusion Method. Various error diffusion algorithms are available. The widely used methods are Floyd Steinberg Half toning algorithm, Jarvis Halftoning algorithm, Stucki Halftoning algorithm. Here halftoning by error diffusion was used and a new algorithm was developed to make a better quality halftone image.

C. Floyd Steinberg Half toning

Nisha Menon K and Minu Kuriakose [9] proposed a method that overcame pixel expansion and loss of contrast by applying halftoning method using Floyd Steinberg algorithm. Here, the hidden image was decrypted by the human vision, only when the correct key image is used. The algorithms used here were Simple Block Replacement (SBR), Balanced Block Replacement (BBR), and Modified Simple Block Replacement (MSBR).

D. Encryption using Digital Watermarking

Pranesh Kulkarni and Girish Kulkarni [10] used Watermarking technique for encryption. Here, one of the shares was embedded with Discrete Wavelet Transform (DWT), and other share was enrolled with Trusted Authority script has been destroyed then the information that had been sent could be considered as lost or irrevocable.

I. Block Based Tranformation

The Rajinder Kaur, Er. Kanwalpreet Singh [14] proposed an algorithm which partitions the image in to random number of blocks with predefined most extreme and least number of pixels, resulting in a stronger encryption and a decreased correlation. Block based encryption and decryption algorithm depends on the combination of image transformation (TA). The secret image was obtained by XOR operation. In addition to the above mentioned methods, other methods were also used specifically to encrypt medical images like X-Rays, CT scan, MRI scan, etc.

E. Quantum Cryptography

To establish a secure transaction of medical image and to detect if any eavesdropping had occurred, Alowolodu [5] used Quantum N Shor's factorizing algorithm. Though this method promotes integrity of the process, there is a troublesome of change in polarization of photons while travelling through the channel. The quantum cryptography is used for securing files (text and images) in a medical environment, which ends up promoting integrity of the profession and puts some assurance of no eavesdropping.

F. Chaos based Quantum Encryption

For the transmission of quantum medical images, Ahmed A. Abd EL-Latif et al.., [11] proposed a method which had higher efficiency when compared with its classical counterpart. The encryption was done by using Novel Enhanced Quantum Representation (NEQR), Gray Code, Bit-plane, Controlled NOT operation and the Chaotic Map. Though it is highly efficient, the cost of replacement of hardware components in case of failures, is high.

G. Encryption based on Irrational numbers

Ranjith Kumar M, Viswanath MK [12] implemented a new encryption scheme using Irrational numbers that secure against all known standard attacks. Here, the transmission was robust. Algorithms such as Fermat's two square theorem, Moore – Penrose inverse, XOR mod operation and Irrational numbers were used in which the key was dynamic. But when using XOR operation, a key is need to set as long as the length of the message. Only then, the encryption will be unbreakable.

H. Combination of Cryptography and Steganography

Steganography is the system of hiding the data within an ordinary file in order to avoid detection. Jamal N. Bani Salameh [13] combined the Modified Jamal Encryption Algorithm (MJEA) for Cryptography and Bit by Bit XORing for Steganography to recover the original image without any loss. The main concern in steganography is, if the decrypting

followed by encoded images and image estimations of correlation, entropy and histograms will be utilized to measure the security of the original image, transformed images, encoded images and decoded image using the combination technique.

J. Particle Swarm Optimization (PSO) Based Image Enhancement

M. Mary Shanthi Rani and G. Germine Mary [15] used PSO algorithm to avoid pixel expansion in decoded image by

subjecting the VC shares to PSO based image enhancement method. Here, no mathematical operation is expected to uncover the secret. Using PSO they decreased the pixel expansion and upgraded the quality of decrypted image.

K. A Simple Visual Secret Sharing Scheme Employing Particle Swarm Optimization

Surya Sarathi Das et al.., [16] proposed a new visual cryptography scheme for grayscale image that utilize Particle Swarm Optimization (PSO) where shares were created gradually through various cycles from the input secret image by contrasting the image with resultant image. But, past research works are nearly confined to binary images by expanding the pixels. Here, PSO was utilized to visually encrypt grayscale image. It was quick, straightforward and also no need of pixel expansion while generating shares. In this way, PSO technique empowers to effectively implement for grayscale image without converting the grayscale image to binary image.

Thus the various techniques and algorithms proposed by different authors in Visual Cryptography are discussed briefly.

Table 1. Recent Research Works In Visual Cryptography

Authors	Technology or Method used	Contribution	Limitation
Nikhil C. Mhala et al.., 2018[7]	Randomized visual secret sharing (RVSS) and discrete cosine transform (DCT)	This method re-establishes the secret image with great differentiation and quality with no leakage of data from any shares. This accomplishes a differentiation level of 70–90% for noise-like and 70–80% for meaningful shares.	This technique faces the problems in pixel expansion and the generation of colored shares is not possible.
Kirti Rawat, 2018[8]	Error diffusion method	The error diffusion method used in the advanced half toning process has minimized the image distortion which provides high security. In this, all the process occur very fast and also maintains the image quality.	Causes lack of sharpness specially at edges in its general form and Correlated artifacts specially seen in constant gray regions
Nisha Menon K, Minu Kuriakose, 2015[9]	Floyd Steinberg Half toning and Block Replacement algorithms	An effective Half toning by Floyd Steinberg error diffusion is used. It can improve the contrast of the image. By pre-processing of halftone images, using block replacement algorithms, the pixel expansion is cancelled.	Excessive memory needs for intermediate image
Pranesh Kulkarni, Girish Kulkarni, 2018[10]	Digital watermarking in discrete wavelet transform(DWT)	Here, one of the shares embedded in the low frequency area of DWT and the other share is enrolled with the Trusted Authority (TA). The secret image is obtained by performing XOR operation on the two shares. This fulfills the robustness, imperceptibility, blindness and security properties.	Its discretization, the discrete wavelet transform (comp. efficient), is less efficient and natural. It take some energy to invest in wavelets to become able to choose the proper ones for a specific purpose, and to implement it correctly.
Olufunso Dayo Alowolodu, 2018[5]	Quantum cryptography, Modified Shor's Algorithm along with Data Encryption Standard (DES)	The quantum cryptography with the use of Shor's Algorithm is used for securing files (text and images) in a medical environment, which ends up promoting integrity of the profession and puts some assurance of no eavesdropping.	Change In polarization of photons while travelling through the channel.

Ahmed a abd el-latif et al.., 2018[11]	Robust encryption in Quantum images	Here, the patient images in one location are transformed into an NEQR representation before being encrypted. For performance analysis, various simulations and numerical methods are employed such as correlation, Shannon Entropy, sensitivity analysis, and histogram analysis.	Failure of hardware components may occur, and it costs high to replace it.
Ranjith Kumar M, Viswanath MK, 2018[12]	Fermat's two square theorems, Moore-Penrose inverse, XOR mod operation, Irrational number	This scheme employs the linear transformation to scramble the positions of image pixels and uses XOR-plus-mod operation increases its resistance to various attacks. It maintains image quality and does not have any mathematical complexities.	When using XOR operation, the key should be as long as the length of the message.
Jamal N. Bani Salameh, 2018[13]	Combination of Cryptography and Steganography, Modified Jamal Encryption Algorithm(MJEA)	The usage of steganography technique followed by encryption by using MJEA results in a lower correlation and higher entropy compared to using encryption alone.	The main disadvantage of steganography is difficult to detect. If the size of original file is already known, then that could be a potential threat to the excess of memory.

The table 1 shows a comparative study of the various technologies, methods and algorithms used in visual cryptography and their limitations.

IV. OPTIMIZATION TECHNIQUES USED IN VISUAL CRYPTOGRAPHY

A technique can be considered to be efficient, only when it is said to be optimized. In order to find some best solution on the basis of certain criteria, we go for Optimization [17]. The Optimization can be achieved using various approaches, but the effective optimization can be achieved by using Bio-inspired algorithms.

a. Bio-Inspired Algorithms

The main challenges of the visual cryptographic techniques used in medical image encryption are, the algorithms used must be most suitable, accurate, faster and robust.

The Biological system is naturally capable of adapting to the changes by learning. Imposing these systems into algorithms is called Bio- inspired algorithms [18]. It involves the concepts like genetic evolution, animal behaviors, social behavior, connectionism, etc.

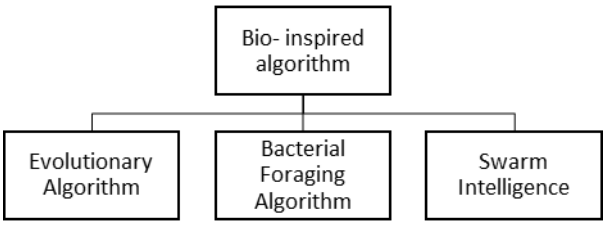

Figure. 2. Three main branches of Bio- inspired algorithm

i. *Evolutionary Algorithm:* Evolutionary Algorithm [19] is used to solve complex problems like, the individuals in a population continuously compete with each other in the process of searching for optimal solutions.

ii. *Bacterial Foraging Algorithms:* Bacterial Foraging[17][18][19] Algorithms inherit the characteristics of bacterial foraging patterns such as chemo taxis, metabolism, reproduction and quorum sensing.

iii. *Swarm Intelligence*: Swarm Intelligence[15][16][19] is designed based on collective behavior of decentralized, self-organized systems that can be either naturally or artificially. It involves operations like separation, alignment, cohesion, etc.

Therefore, Swarm Intelligence can be considered to be the most appropriate methodology for image processing.

b. Areas of Image Processing

In the field of Image Processing, Bio- inspired algorithms are used in the following areas [19].

1) Image segmentation
2) Feature extraction
3) Image enhancement
4) Image registration

i. Image segmentation: Image segmentation is the process of splitting the digital image into multiple segments (set of pixels). The main objective of segmentation is to simplify or modify the image representation, which will be more meaningful and easier to analyse.

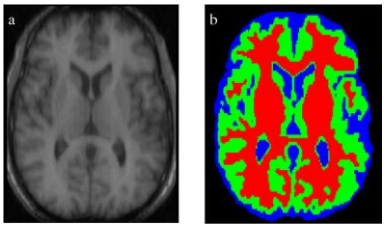

Figure.3. Segmentation of XRAY Image

ii. Feature extraction: Feature extraction is basically a reduction process, where an image is reduced to a more manageable one for processing, where the reduced image will still describes the initial image accurately and completely.

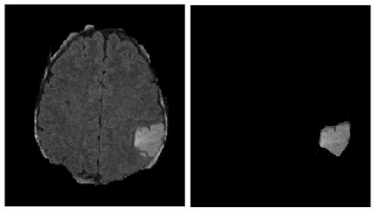
Figure.4. Extraction from MRI image

iii. Image enhancement: Image enhancement is the process of improvising the quality of digital image using certain software. Here, the various properties of an entire image or a part of the image is modified to enhance the quality.

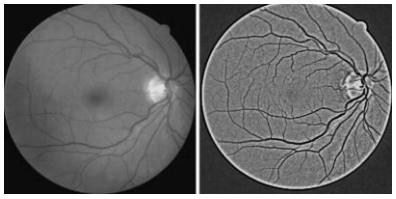
Figure.5. Enhancement of Iris image

iv. Image registration: Image registration is the process of fusing two or more images to provide more information. This combination of images refers to the fusion of images obtained from various imaging equipment or sensors.

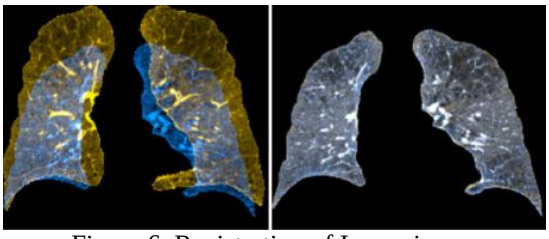
Figure.6. Registration of Lungs image

Table.2. Comparison of Research Works Using Visual Cryptography Parameters and Implementation Environment

Methods	Input Image	Share Type	PSNR	WSNR	MSE	LDM	UQI	Implementation Environment
Randomized Visual Secret Sharing Encryption [7]	Both	Both	✓		✓			Simulation
Error Diffusion Method [9]	Grey	Noise like shares	✓				✓	Simulation
Encryption using Digital Watermarking [15]	Grey	Meaningful	✓		✓			Simulation
Quantum ,Cryptography [16]	Both	Meaningful						Proposed in real time application and Simulated
Combination of Cryptography and Steganography [19]	Both	Meaningful	✓		✓			Simulation
Chaos based Quantum Encryption [17]	Grey	Noise like shares	✓				✓	Proposed in real time application and Simulated
Jarvis	Grey	Noise like	✓	✓		✓	✓	Simulation

Algorithm [9]		shares						
Stucki Algorithm [9]	Grey	Noise like shares	✓	✓		✓	✓	Simulation
Encryption based on Irrational numbers [18]	Colored	Meaningful	✓				✓	Simulation
Floyd Steinberg algorithm [9]	Grey	Noise like shares	✓	✓		✓	✓	Simulation

From the table 2, we infer that

- Most of the visual cryptography techniques use grayscale images than coloured images as the input image during encryption.
- Though some techniques use input as coloured images, initially they undergo the process of converting that coloured imageinto grayscale binary image, then it is processed further.
- When the meaningful shares are used, the encryption of the images can be done efficiently rather than using the noise-like shares
- Most of the visual cryptography techniques consider the common parameters like PSNR and MSE for evaluating the quality of the image gained.
- Other parameters like WSNR, UQI and LDM are rarely considered.
- Many methods are not implemented directly in practical cases, only the simulation is shown by using the software like MATLAB.

V. DISCUSSION

From the analysis of different methodologies and techniques, we infer that,

- It is hard to evaluate the accurate significance of the visual cryptographic techniques since most of them are not implemented in real time cases.
- The usage of bio inspired algorithms for the purpose of optimization during the initial stages of half toning process in the visual cryptography will yield a better quality of obtained image and a better PSNR ratio which will make the entire process into an efficient one.

VI. CONCLUSION

The security of medical images during the transmission over a network is very important. This paper describes the several techniques used to secure the medical images using visual cryptography. The different types of methods and techniques used, their efficiency and their drawbacks are discussed in detail. The overall analysis of the degree of security and the parameters used in each technique is also provided. An overview about the bio inspired algorithms used for the purpose of optimization is discussed and also a better usage of these bio inspired algorithms in the stages of visual cryptography methodology is also suggested.

REFERENCES

[1] M. Naor and A. Shamir, "*Visual cryptography. Advances in Cryptology*" EUROCRYPT '94. Lecture Notes in Computer Science, pp:1–12, 1995

[2] R.Youmaran et al.., "An Improved Visual Cryptography Scheme for Secret Hiding" 23rd Biennial Symposium on Communications, 2007

[3] Shruti M. Rakhunde Manisha Gedam, " Survey on Visual Cryptography: Techniques, Advantages and Applications", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661

[4] Anjney Pandey and Subhranil Som " Applications and Usage of Visual Cryptography: A Review" ICRITO, Vol.978, Issue.1, pp.5090-1489-7, 2016

[5] Alowolodu et al.., "*Medical image security using quantum cryptography. Issues in Informing Science and Information Technology*", Vol.15, pp.57-67, 2018

[6] Digvijay Singh, Pratibha Sharma " *Comparison of various Error Diffusion Algorithms Used in Visual Cryptography with Raster scan*" IJEDR, Vol. 5, Issue 2 , ISSN 2321-9939, 2017

[7] Nikhil C. Mhalal et al.., *" Randomised visual secret sharing scheme for grey-scale and colour images*", ISSN 1751-9659 Accepted on 29th October 2017 E-First on 9th January 2018

[8] Kirti Rawat, "*An Approach for Grey Scale Image in Visual Cryptography Using Error Diffusion Method*" IJCST – Vol. 5 Issue 3, ISSN: 2347-8578, 2017

[9] Nisha Menon K, Minu Kuriakose "*A novel visual cryptographic scheme using Floyd Steinberg halftoning and block replacement algorithms*" IJARBEST journal Vol. 1, Issue 1, 2015

[10] Pranesh Kulkarni, Girish Kulkarni " *Visual Cryptography based Grayscale Image Watermarking in DWT domain*" Proceedings of the 2nd ICECA, ISBN:978-1-5386-0965-1, 2018

[11] Ahmed a. Abd el-latif et al.., *" Robust Encryption of Quantum Medical Images* ", IEEE Vol. 6, pp. 2169-3536, 2018

[12] Ranjith Kumar M and Viswanath MK " *A symmetric medical image encryption scheme based on irrational numbers* " Biomedical Research; Special Issue: S494-S498 ISSN 0970-938X, 2018

[13] Jamal N. Bani Salameh *" A Secure Transmission Approach for Medical Images and Patient's Information by Using Cryptography and Steganography* " IJCSN - International Journal of Computer Science and Network, Vol. 7, Issue 5, ISSN: 2277-5420, 2018

[14] Rajinder Kaur et al.., " *Comparative Analysis and Implementation of Image Encryption Algorithms*", IJCSMC, Vol. 2, Issue. 4, pg.170 – 176, ISSN 2320–088X, 2013

[15] M. Mary Shanthi Rani and G. Germine Mary, "*Particle Swarm Optimization Based Image Enhancement of Visual Cryptography Shares*", Springer International Publishing Switzerland, Vol. 14, No. 9, ISSN 1947-5500, 2017

[16] Surya Sarathi Das et al.., "*A Simple Visual Secret Sharing Scheme Employing Particle Swarm Optimization*", CIEC, Vol.978, Issue.1, pp.4799-2044-0, 2014
[17] D. Oliva and E. Cuevas, "*Advances and Applications of Optimised Algorithms in Image Processing*", Springer International Publishing AG 2017. doi 10.1007/978-3-319-48550-8_2
[18] K. K. Mishra and Shailesh Tiwari and A. K. Misra, "*A Bio Inspired Algorithm for Solving Optimization Problems*", ICCCT, Vol.978, Issue.1, pp.4577-1386-611, 2011
[19] Noor Elaiza Abdul Khalid et al.., " *A Review of Bio-inspired Algorithms as Image Processing Techniques*", ICSECS, Part I, CCIS 179, pp. 660–673, 2011

Authors Profile

Dr. C. Punithadevi pursed Bachelor of Science from Bharathidasan University, Puducherry in 1996 and Master of Computer Application from Bharathidasan University in year 1999. She pursued M.Tech in the stream of Computer Science and Engineering from Pondicherry University in 2007 and completed Ph. D in the stream of Computer Science and Engineering from Pondicherry University in 2015. She is currently working asProfessor in Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry since 2015. Her research area based on Service Orientation Architecture, Information Integration and Software Architecture. She has 13 years and 7 months of teaching experience and 4 years and 6 months of Research Experience.

Ms. Thenmozhi. B is currently pursuing the last year of her undergraduate degree in Bachelor of Technology in the stream of Information Technology in Sri Manakula Vinayagar Engineering College, Pondicherry University, Pondicherry, India. She will complete her degree by May 2019. As a part of her B.Tech project she and her group mates have implemented this paper. She is interested in the areas of Cryptography and Networking.

Ms. Raga. G is currently pursuing the last year of her undergraduate degree in Bachelor of Technology in the stream of Information Technology in Sri Manakula Vinayagar Engineering College, Pondicherry University, Pondicherry, India. She will complete her degree by May 2019. As a part of her B.Tech project she and her group mates have implemented this paper. She is interested in the areas of Networking, Web Technology and Database management systems.

Ms. Kreethika Jain is currently pursuing the last year of her undergraduate degree in Bachelor of Technology in the stream of Information Technology in Sri Manakula Vinayagar Engineering College, Pondicherry University, Pondicherry, India. She will complete her degree by May 2019. As a part of her B.Tech project she and her group mates have implemented this paper. She is interested in the areas of Computer Networking.

