International Journal on Advances in Engineering Technology and Science
Volume: 5, Issue: 2, 2024, e-ISSN: 2455-3131
DOI: 10.5281/zenodo.12571247

A Detailed Survey on Visual Cryptography Color Images for Cloud Storage

Rakesh Kumar Verma[1], Daya Shankar Pandey[2], Varsha Namdeo[3]

Computer Science & Engineering, Sarvepalli Radhakrishnan University, Bhopal

[1]rakeshvermabplsrk@gmail.com, [2]dayashankar.rkdfist@gmail.com, [3]varsha_namdeo@yahoo.com

***Abstract* – It is a high concern to secure huge amount of imaging data stored over the cloud servers. The Visual Cryptography (VC) is a widely used approach to encrypt these imaging data. VC is a powerful technique in which a secret image can be divided into two or more shares and the decryption can be done using human visual system. The VC may understand as crypto sharing approach for embedding true crypto image information to the transparency ciphers. VC has wide range of applications like in biometrics, print online banking, cloud computing, internet voting, etc. In VC a secret image is hidden into two or more shares which on superimposing will recover the hidden image. There are many algorithms designed for VC to secure the images. A related survey has been done in this paper on various visual cryptography schemes based on the number of secrets, pixel expansion, type of share generated, image format, and number of secret images. Paper also presents a detailed review about various visual cryptography color images for cloud storage.**

Keywords – Visual Cryptography, Image, Security, Halftoning, Multi-Share, Encryption, Cloud.

I. INTRODUCTION

Visual cryptography (VC) is a process of encrypting the images utilizing the secret shares generations [1]. Visual cryptography is a secret sharing plan that partitions secret images into shares to such an extent that, when the shares are superimposed, a hidden secret picture is uncovered. VC was first proposed in 1994 by Naor and Shamir. It is a secret sharing plan, in view of highly contrasting or binary images [2]. VC is a worldview in which a secret picture is changed over into at least two good for nothing, non-indistinguishable shares, without utilizing any encryption keys [3]. The hidden secret can be uncovered just when the shares are stacked together. Secret images are separated into share images which, all alone, uncover no information of the original secret. Shares might be circulated to different parties so that exclusively by working together with a fitting number of different parties, can the subsequent joined shares uncover the secret picture [4]. The magnificence of VC lies in the realities that the hidden secret can never be recuperated just by having one of the shares, and furthermore that the secret can be uncovered with practically no computer intervention [5]. This permits VC to be utilized by anybody with practically no profound comprehension of cryptography, and with next to no hard computations. VC is not quite the same as the standard cryptographic secret sharing [6]. In cryptographic secret sharing technique, every participant is permitted to maintain a piece of the mystery which could be uncovered without any problem. However, this inconvenience is overwhelmed by the VC as it utilizes concealing secrets into multiple shares which never uncover the secret until stacked together [7].

The secret recovery is as simple as superimposing transparencies containing the shares, which allows the secret to be reconstructed. VC is a desirable scheme as it embodies both the scheme of perfect secrecy and a very simple mechanism for recovering the secret [8]. Figure 1 represents the basic model of VC scheme. While considering popular cryptographic schemes which are conditionally secure, VC provides robust security to the secret image. This makes VC suitable for highly sensitive applications like biometric authentication, secure electronic ballots, safe online banking, digital watermarking, and security against DoS attacks in WiMax authentication system etc [9].

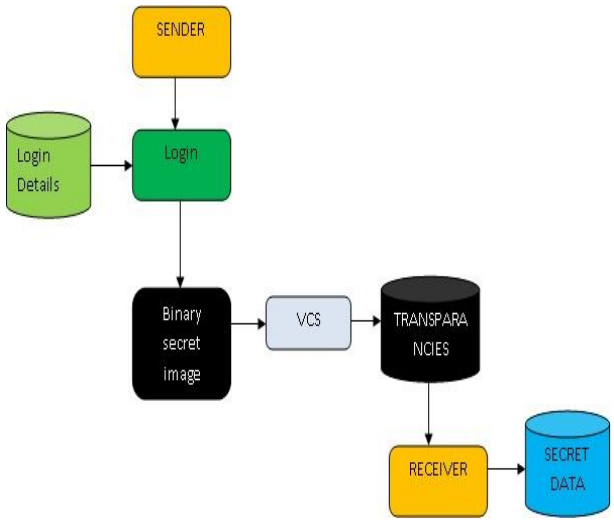

Fig.1- Model of Visual Cryptographic Scheme

Regaining of the secret should be possible by super-forcing the offer images and, consequently, the decoding system requires no unique hardware or software and can be just finished by the natural eye. Visual cryptography (VC) is specifically noteworthy for security applications dependent on biometrics [10]. VC permits us to effectively and efficiently divide secrets among various trusted parties or users and storage areas like cloud. Similarly, as with numerous cryptographic plans, trust is the most troublesome aspect. Visual cryptography gives an exceptionally amazing technique by which one secret

can be dispersed into at least two shares. At the point when the shares on transparencies are superimposed precisely together, the original secret can be found without computer investment [11].

II. Types Of Visual Cryptography Algorithms

Many kinds of visual cryptography are analyzed that is from the absolute first kind of traditional visual cryptography straight up to the most recent turns of events. Traditional VC explicitly deals with sharing a single binary secret among various participants [12]. The VC utilizing random grids is another to that of the traditional VC as it diminishes the issue of pixel expansion. Segment-based VC is one more methodology which can be utilized to encrypt numbers. Extended VC endeavours to make this a stride further by presenting shares that have critical visual importance. This reduces the dubious looking encrypted shares that are produced utilizing the traditional VC. MIVC permits encryption of more than one secret picture. Moderate VC discharges the secret logically [13]. Moire's cryptography and picture hatching VC plans is a portion of different turns of events. Halftoning techniques have been informed which makes VC to be utilized on color and grayscale images. The grayscale and color images can likewise be an input to all the VC plans [14].

Visual Cryptography Schemes (VCS) are arranged into two fundamental classes that are shown in figure 2.

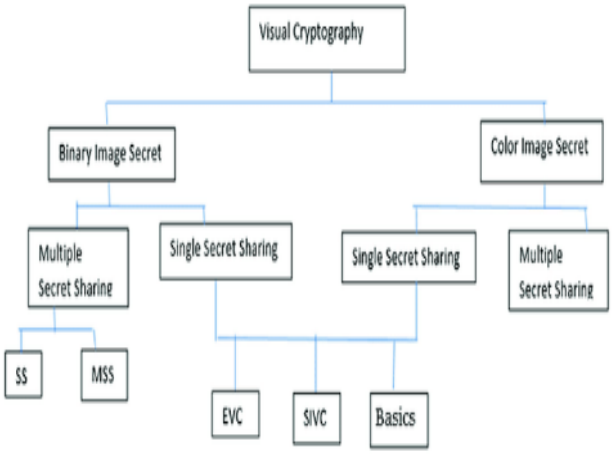

Fig.2- Classification of visual cryptography

- Binary secret sharing plans that arrangement with high contrast secrets and
- Color secret sharing plans managing colored just as dim level secret images.

Every one of the two classifications is additionally arranged into Single Secret Sharing (SSS) and Multiple Secret Sharing (MSS).

- The SSS, in the two classifications, is isolated into three gatherings;
- Extended visual cryptography (EVC) where the shares have a significance view,
- Size invariant Visual Cryptography (SIVC) where the size of the recovered picture is a similar size of the first one, and
- Basic schemes which have some unique qualities.

In binary classification, Multiple Secret sharing is divided into two subgroups:

- Standard Secret sharing (SS) and
- Master Share Secret sharing (MSS)

Visual Cryptography Scheme for Binary images- All past visual cryptography plans was simply restricted to binary images. These techniques could do procedure on just highly contrasting pixels. It isn't adequate for genuine applications. In this plan a vacillating technique is utilized to change over dark level picture into surmised binary picture. Then, at that point, existing visual cryptography plans for binary images are applied to make the shares [15].

Visual Cryptography Scheme for Color images- Visual cryptography plans were applied to just highly contrasting images till year 1997. In this visual cryptography conspire one pixel is disseminated into m sub pixels, and each sub pixel is separated into c color regions. In each sub pixel, there is by and large one-color locale colored, and the wide ranges of various color regions are dark [16].

Single Secret Sharing (SSS) - For sharing a secret color picture and furthermore to produce the significant offer to communicate secret color picture, color visual cryptography plot was expected. For a secret color picture two critical color images are chosen as cover images which are a similar size as the secret color picture. Then, at that point, as per a predefined Color Index Table, the secret color picture will be hidden into two disguise images. One disservice of this plan is that additional room is needed to collect the Color Index Table. In this plan additionally number of sub pixels is in corresponding to the quantity of colors in the secret picture [17].

Multiple Secret Sharing (MSS) - All the past explores in visual cryptography were centered on securing just each picture in turn. Wu and Chen were first analysts, who fostered a visual cryptography plan to share two secret images in two shares. In this plan, two secret binary images can be hidden into two random shares, specifically An and B, to such an extent that the principal secret can be seen by stacking the two shares, signified by A⊗ B, and the subsequent secret can be acquired by rotating A by 90 degrees against clockwise. J Shyu et al. proposed a plan for a considerable length of time sharing in visual cryptography, where beyond what two secret images can be secured at a time in two shares [18].

Extended visual cryptography (EVC) - In traditional visual cryptography plot, shares are made as random patterns of pixel. These shares resemble a noise. Noise-like shares stimulate the consideration of hackers, as hacker might speculate that a few data is encrypted in these noise-like images. So it becomes inclined to security related issues. It likewise becomes hard to oversee noise-like shares, as all shares resemble the other the same. An extended visual cryptography (EVC) gives techniques to

make significant shares rather than random shares of traditional visual cryptography and help to stay away from the potential issues, which might emerge by noise-like shares in traditional visual cryptography [19].

Size invariant Visual Cryptography (SIVC)- This plan eliminates the requirement for the pixel expansion. This prompts more modest shares which are nearer to the secret picture size. SIVC decreased the quantity of additional sub-pixels expected to uncover the secret. Thus, the size of shares will be diminished to be a similar size of the secret picture which keeps away from distortion while recreating the secret. Another scientist likewise proposed a SIVC plot that decreased the distortion while decrypting the secret picture [20]. Their plan has a wide scope of down to earth applications, for example, authentication with steganography and bamboozling counteraction plans. In any case, there is likewise a need to develop the nature of the recovered picture as far as contrast [21].

III. HALFTONE VISUAL CRYPTOGRAPHY

The VC techniques talked about so far are material to binary images as it were. To stretch out these strategies to be appropriate to grayscale and color images, a pre-processing technique is required. This pre-processing technique is called halftoning technique. Halftoning is a reprographic technique that simulates continuous tone imagery using dots, shifting either in size or in spacing, in this manner producing a gradient-like effect. The continuous tone imagery contains an endless scope of colors and grays. The halftone interaction diminishes visual reproductions to a picture that is turned out with just one color of ink, in dots of contrasting size or spacing. These small halftone dots are blended into smooth tones by the human visual framework.

Except from halftoning, Moire's pattern, turbulent planning and dark level relative contrast can be utilized for applying VC on grayscale images. Essentially, picture hatching technique can be utilized to apply VC on color images.

There are a few kinds of halftoning techniques. This subsection audits approaches of the halftoning techniques to create "Blue Noise" for results of good visual quality halftoning pattern. In PC designs the term of "Blue Noise" produces stochastic vacillate pattern equivalent to the size of dots and circulated dots as homogeneously and irregular way as could be expected. The name of Blue Noise alludes to phantom substance of these patterns; it is formed absolutely from "high-frequency" part with insignificant low frequency parts. Halftone technique is ordered into three classifications as displayed in fig 3, this large number of classes corporate with (HVS) gadgets.

Halftone utilizing Error Diffusion (E-D) - Error Diffusion algorithm is neighbourhood processor that endeavours to deliver "Blue Noise ". E-D is generally effective and most straightforward innovation of halftone algorithms. In this strategy, it spreads the quantization error to neighbour of the handled pixel. The quantization error isn't relied on just the current input and output esteems yet additionally the whole previous history. The design of E-D filter is to limit the "low frequency" between the source picture and target picture.

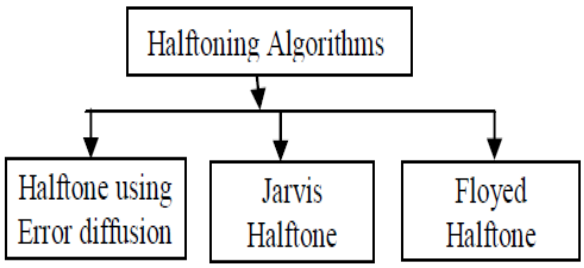

Fig.3- Types of halftoning techniques

Figure 4 outlines binary E-D filter block graph to change over the continuous – tone input picture to binary output picture that comprises just of [0,1]. Where f(m,n) represents to current handled pixel , d(m,n) is the amount of the f(m,n) pixel and "diffused" past errors , g(m,n) is output quantized pixel esteem. E-D algorithm is made of two essential components.

i) Threshold block where the output g(m,n) can be calculated by

$$g(m,n) = \begin{cases} 1, & \text{if } d(m,n) \geq t(m,n) \\ 0, & \text{other wise} \end{cases}$$

The threshold t(m,n) can be position-subordinate.

ii) The error filter h(k,l) whose input e(m,n) is the contrast between

d(m,n) and g(m,n) . At last, d (m,n) can be calculated as:

$$d(m, n) = f(m,n) - \sum_{k,l} h(k,l)e(m-k, n-l)$$

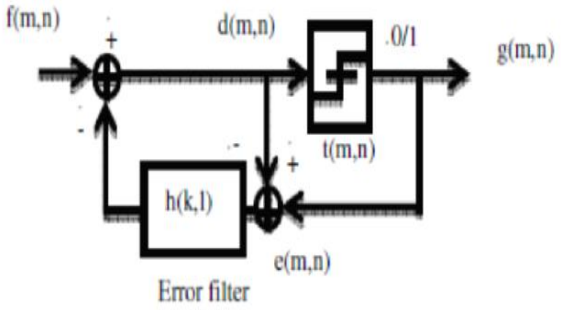

Fig.4- Block diagram of Binary Error Diffusion

Jarvis halftoning algorithm- This algorithm proposed by J.F. Jarvis, C.N. Judice and W. H. Ninke, it is portrayed by utilizing diverse error diffusion matrix from Floyd and Steinberg which is more complicated however makes more extensive error distribution, so this algorithm is less quick. Jarvis diffusion quantization error to 12 adjoining pixels agreeing (Jarvis) error coefficient matrix as displayed in figure 5. The output picture of this algorithm is displayed in figure 6.

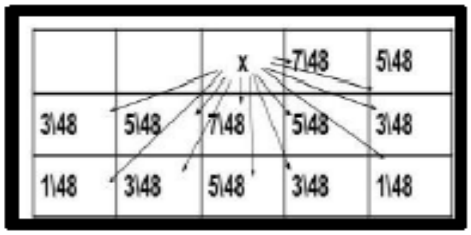

Fig.5- Jarvis error diffusion matrix

Fig.6- Output image of (Jarvis) halftoning algorithm

Floyd halftoning algorithm

This algorithm, which is first proposed by Floyd and Steinberg, flows the quantization error of current interaction pixel to four neighbour pixels is finished by utilizing the error diffusion matrix displayed in figure 7 (where X is current cycle pixel).

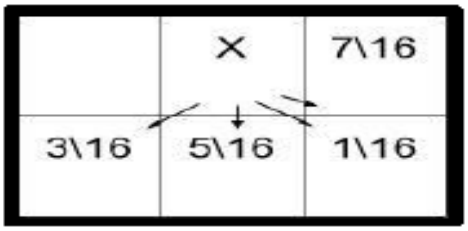

Fig.7- Floyd error diffusion matrix

The Floyd - Steinberg E-D filter of gray level pattern is quicker algorithm however finish from directional "Worm" antiques. The output picture of this algorithm is displayed in figure 8.

Fig.8- Output image of Floyd halftoning algorithm

Summary of some VC techniques are discussed in the table1.

Table-1: Summary of some VC techniques

Authors and Year	VC-Techniques	Performance	Typical applications
J. Mahalakshmi and K. Kuppusamy, 2016	Cipher block chaining for RGB based encryption	Their outcomes uncover that the technique serves not just better for RGB image encryption and furthermore opposes to different cryptanalytic assaults.	Secures the mages for cloud computing.
J. Tamilarasi et al. 2014	Halftone based two share-based VC	Their algorithm brings some noise into the recovered image; still that image is generously clearer than in other proposed non-extension algorithms.	Applied to both binary and halftone images.
Anuja Dagar et al. 2012	Halftone based on Floyd Steinberg Dithering	Their method is designed for higher computing performance. Their algorithm is based on error dispersion and commonly used by image manipulation software like when an image is converted into GIF format.	Used in mobile communication devices as multi core architecture
Bharati Pannyagol in 2014	Jarvis Error diffusion and VIP Synchronization	Their experimental results show that shares are meaningful color shares and the stacked images have good visual quality. And hence the error diffusion and VIP synchronization improve the visual quality of shares and stacked images.	Used for visual cryptography for color Images.
Kirti & Singara, 2017	Two extended visual cryptography (EVC) Techniques	Their techniques take less time to implement which makes them applicable to real time systems.	Used to share images like medical, geographic maps, special and satellite images.
M. Bharathi et al. 2013	Visual halftoning	Their method takes advantages of VC by using shares for image watermarking. The random noise like patterns is generated using secret of binary images.	Used for the generation of image watermarking.
M. Karolin et al. 2019	Share1 and share2 are Encrypted and decrypted using Blowfish algorithm.	They demonstrated that using the multiple shares can enhance the security of the images.	Used to secure the transmitted images
Yu-Xia Sun et al. 2019	A reversible data hiding (RDH) scheme in encrypted color halftone images (RDH-ECH).	They have concluded that the original image can be restored entirely after the watermarks are extracted. Besides, for marked color halftone images, their algorithm can implement high	Used to data hiding applications such as the healthcare industry and online distribution

		embedding capacity and moderate visual quality	systems.
Ms. Shital B Patel1, Dr. Vinod L Desai, 2018	Error diffusion method.	The recovered secret image (share) are better quality means better secret hiding and for better secrecy. Their technique increases the overall performance of visual cryptography.	Used in the field of Biometric security, Watermarking, Remote electronic voting, Bank customer identification etc.

IV. VISUAL CRYPTOGRAPHY METRICS

Here, we are discussing some relevant metrics that are commonly used to evaluate or describe them. We will discuss each of them individually in this subsection.

Pixel expansion- It defines the number of sub-pixels m in produced shares that address a solitary pixel in a unique image. This boundary presents in loss of resolution from a unique image to share image in VC methodology. At the point when the shares are covered the recuperated image won't be of a similar quality of unique image. The recuperated image has less contrast and encounters a deficiency of resolution when contrasted with secret image.

Contrast- It is the overall difference among high contrast pixels of a binary image or the difference in shading tones in colored images. It reflects upon the clearness or sharpness of a specific image. For VC schemes, the contrast of recuperated (decrypted) images is determined as a proportion of quality. As a rule, the VC encryption and decryption process prompts a misfortune in contrast.

Security- It alludes to the measure of information about the secret image that can be extricated from share images. The recuperated image ought not be uncovered with under (k−1) shares in (k, n) schemes. The security boundary is by and large fulfilled when the strength of an encryption interaction (share generation) keeps an intruder from removing pieces of information about the secret image.

Complexity- It can be isolated into two kinds: computational and memory complexity. Computational complexity is worried about the quantity of absolute activities (time) needed to produce the arrangement of shares n, and to recreate the secret image. Memory complexity alludes to the measure of storage (memory) needed for a VC conspire. Complex VC calculations have higher computational and memory complexity, which then, at that point, requires all the more remarkable hardware to execute. This might deliver specific framework unacceptable for high speed, constant choices.

Type of shares of a VC scheme- It can either be meaningless or meaningful. A meaningless share looks like clamor though a meaningful share is a detectable image used to insert information from the secret image. Contingent upon the application, the utilization of either might be liked. For instance, a meaningless share might stir the doubt of an enemy while a meaningful share may not.

Number of secrets- It is the quantity of secret images that are encrypted by a VC strategy. When there are different secrets, the secret images are totally encrypted into similar arrangement of shares. Decryption process is performed by covering shares that are turned or flipped to recuperate different secret images.

Accuracy- Accuracy of a VC scheme measures the quality of a recuperated image. In a perfect world, the recuperated image ought to be a precise imitation of the first secret image. The objective of any VC plot is to augment accuracy, which can be assessed by PSNR, mean square mistake (MSE), and CC measurements.

V. VISUAL CRYPTOGRAPHY OVER CLOUD COMPUTING

Images are turning into an inescapable piece of knowledge in the advanced society. As the world changes, the innovation is likewise evolving quickly. Different confidential data like clinical images, biometric images, space and geographical images taken from satellite and business significant document are transmitted over the Internet and put away in far off areas for future access. The everyday requirements for computing resources are expanding. As data is developing at a quick rate, costs engaged with putting away and keeping up with data is additionally rising quickly. The best substitute solution to lessen the storage cost is re-appropriating every one of the data to the cloud.

Cloud computing has turned into a promising innovation for obtaining computing and storage resources on request. Cloud permits customers to keep their services exceptionally accessible with reasonable rate: the customers just need to sequestrate the storage service and pay for the specific measure of utilized storage; clients in like manner can approach this data anytime/anyplace. Sadly, somehow or another cloud computing is overwhelmed by the proliferous security danger springing from the numerous sorts of attacks. As the kernel security element, password authentication and image encryption assume an established part in present day computing systems [4].

A. Password Authentication- The most far-reaching authentication plot is textual password. The disadvantages of this plan like eves word reference attack; insider attack, dropping, and social designing are notable. There are a few plans based on producing a random and length password that can make the system safer. In any case, the principal issue is the trouble of recalling those passwords. In the opposite side, there are many examinations clarified that valid clients will more often than not select short passwords that are not difficult to recall.

B. Image Encryption- Image encryption becomes essential applications in the Internet communication, clinical imaging, database the board system, multimedia systems, telemedicine, and so on the security of digital images has

acquired consideration recently, and a few image encryption plans have been introduced to work on the security of images transmission. Image encryption plans expect to change digital image over to another that is hard to comprehend. On the opposite side, image decryption finds the first image from the encoded image.

The general idea of the system is extremely basic and it likewise ensures the secret in the document. For a security reason, rather than uploading the first document file, it should be changed over into a text file, again into an image file and afterward transferred in to the cloud.

Later the downloaded image files should be changed over into a text file and again into the first document file. The accompanying advances are to be performed for uploading a document file (doc/docx) into a cloud and downloading a document file from the cloud.

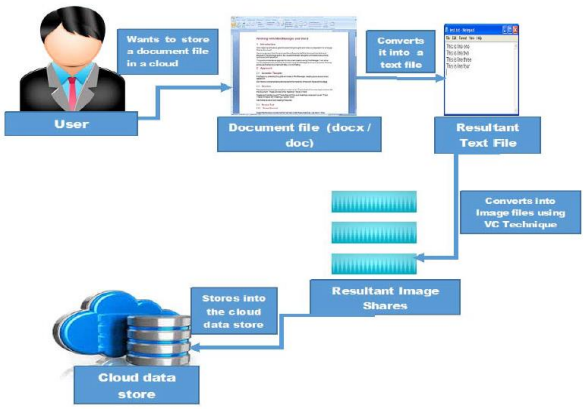

Fig.9- Visual Cryptography over cloud

At the point when the client needs to transfer a document file, which contains some secret information, it should be encoded by this encryption strategy which includes two phases. In the underlying stage the document file should be changed over into a text file using Apache Poi application programming interface and in the following stage the resultant text file should be encoded using SDSUVC encryption procedure. Each line from the text file should be perused and every single person changed over into a whole number (ASCII esteem). A singular pixel should be benefited from a buffered image using SetRGB technique. A line of a pixel should be put away in the primary image and the following one in the subsequent image and the other line in the third image. This interaction is rehashed until the file reaches a conclusion. At long last the shares of the image file should be transferred into a cloud as displayed in Figure 9.

VI. CONCLUSION

VC is a process of encrypting the images using the secret shares generations. There are many VC based algorithms have been designed in the past. The prime goal of the cryptography methods is to generate the unique secret share key. Many key generation algorithms were designed which in turn differentiates the design of VC algorithms. The key or share may be public or private. It is a high concern to design the robust keys or shares. The idea of the VC is to encode or encrypt the cipher image using the secret shares and then it is desired to recover the true cipher image. Out of various schemes some have shown very promising results with or without a small increase in the final image dimension which is also referred as pixel expansion. The proper alignment of the distributed shares reveals the original secret image. In this paper we provide a state-of-the-art review and analysis of the several existing schemes of Visual Cryptography.

REFERENCES

[1] J. Mahalakshmi and K.Kuppusamy, "An efficient Image Encryption Method based on Improved Cipher Block Chaining in Cloud Computing as a Security Service", Australian Journal of Basic and Applied Sciences 2016, pp 297-306.

[2] 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, April 2014, pp 126-131.

[3] Punithavathi P, Geetha Subbiah, "Visual Cryptography for Securing Images in Cloud", IGI Global 2016, pp 242-263.

[4] Ali A.Yassin, Abdullah A. Hussain, Keyan Abdul-Aziz Mutlaq, " Cloud Authentication Based on Encryption of Digital Image Using Edge Detection", IEEE 2015, pp 1-7.

[5] Ali Kadhim Bermani, Mehdi Ebady Manaa , Ahmed Al-Salih, " Efficient cryptography techniques for image encryption in cloud storage", Periodicals of Engineering and Natural Sciences, July 2020, pp 1359-1373.

[6] Nithya Chidambaram, Pethuru Raj, Karruppuswamy Thenmozhi, Rengarajan Amirtharajan, "Advanced framework for highly secure and cloud-based storage of colour images", The Institution of Engineering and Technology 2020 pp 3143-3153.

[7] Vishruti Kakkad, Meshwa Patel, Manan Shah, " Biometric authentication and image encryption for image security in cloud framework", Springer 2019, pp 1-17.

[8] Paul Rad, Mohan Muppidi, Aldo S. Jaimes, Sos S. Agaian, and Mo Jamshidi, " A Novel Image Encryption Method to Reduce Decryption Execution Time in Cloud", IEEE 2015, pp 1-5.

[9] K. R. Sajay, Suvanam Sasidhar Babu, Yellepeddi Vijayalakshmi, "Enhancing the security of cloud data using hybrid encryption algorithm", Springer 2019, pp 1-10.

[10] Mouhib Ibtihal, El Ouadghiri Driss, Naanani Hassan, "Homomorphic encryption as a service for outsourced images in mobile cloud computing environment", International Journal of Cloud Applications and Computing 2017, pp 1-10.

[11] Ijaz Ahmad Awan, Muhammad Shiraz, Muhammad Usman Hashmi, Qaisar Shaheen, Rizwan Akhtar and Allah Ditta, "Secure Framework Enhancing AES Algorithm in Cloud Computing", Security and Communication Networks 2020, pp 1-16.

[12] PengCheng Wei, Dahu Wang, Yu Zhao1, Sumarga Kumar Sah Tyagi, Neeraj Kumar, "Blockchain data-based cloud data integrity protection mechanism", Elsevier 2020, pp 1-12.

[13] Manjit Kaur, Vijay Kumar1, "A Comprehensive Review on Image Encryption Techniques", Springer 2020, pp 2018, pp 1-29.

[14] Miss. Shakeeba S. Khan1, Miss. Sakshi S. Deshmukh, "Security in Cloud Computing Using Cryptographic Algorithms", IJCSMC 2014, pp 517-525.

[15] Mahantesh N. Birje, Praveen S. Challagidad, R.H. Goudar, Manisha T. Tapale, "Cloud computing review: concepts, technology, challenges and security", Int. J. Cloud Computing 2017, pp 32-58.

[16] K. Padmaja and R. Seshadri, "A Review on Cloud Computing Technologies and Security Issues", Indian Journal of Science and Technology, Dec 2016, pp 1-8**.**
[17] May A. Salama, Mona F.M. Mursi, Manal Aly, “Safeguarding images over insecure channel using master key visual cryptography”, Elsevier 2018, pp 1-13.
[18] Suhas B. Bhagate, P.J.Kulkarni, “An Overview Of Various Visual Cryptography Schemes”, International Journal of Advanced Research in Computer and Communication Engineering 2013, pp 3676-3679.
[19] Shruti M. Rakhunde, Manisha Gedam, “Survey on Visual Cryptography: Techniques, Advantages and Applications”, NCRTCSIT-2016, pp 6-12.
[20] Dyala R. Ibrahim, Je Sen, “An Overview of Visual Cryptography Techniques”, Multimedia Tools and Applications, September 2021, pp 1-27.
[21] Sandhya Anne Thomas, Saylee Gharge, “Review on Various Visual Cryptography Schemes”, ICCTCEEC-2017, pp 1164-1167.