Enhancement of Security in Visual Cryptography using DES

Surbhi Bajaj¹, Kamal Khajuri²
Department of ECE
Maharishi Ved Vyas Engineering College, Kuk University, India

Abstract:
As the advancement in the technology increases maintaining the security of visual information during its transaction has to be increased Internet has become most commonly used media for communication and hence text, voice, video, Images and many more are broadcast through Internet. These might include Military Secrets, Commercial Secrets and therefore it has to be transmitted by safer means with improve security. In general, for some critical security issue the visual cryptography scheme is used, VC is the special kind of cryptographic technique in which secret image is encrypted into shares which refuse to disclose information about the original secret image Cryptography in the study of a mathematical techniques related aspects of data security such as confidentially, data safety, entity authentication, but it is neither only the means of providing message security, rather one of the techniques. Visual cryptography can be practiced for copy right for images, as well as access control to user images, visual authentication and identification any type images of images comparable(normal or digital).Visual cryptography is a new technique which grant information security which practiced simple algorithm unlike the complicated, computationally intensive algorithms used in other techniques like traditional cryptography here we are going to implement a (n, n) visual cryptography scheme and method to improve more security to shares, the shares can be encrypted using DES algorithm and addition we present a concise detail about the instructions for future research.

Keywords: Visual cryptography, DES algorithm, stenographic image, PSNR, decryption, secret sharing.

I. INTRODUCTION

Definition
Visual cryptography is a cryptographic procedure which allows visual information to be encrypted in such a manner that the decryption can be done by human cryptography refers to the study of mathematical techniques and related aspects of message security like data confidentiality, data integrity and of data authentication. In the process of Visual Cryptography undisclose image is encrypted into shares which refuse to disclose information about the original secret image. Decryption is through an independent decryption algorithm. A basic model for Visual Cryptography for natural images was suggested by Naor and Shamir, where the resultant image is twice the size of secret image. As the advent of electronic applications boost, providing the security for information in an open network environment is required. Encryption is a process of transforming original data, called plain text or clear text into a form that appears to be arbitrary and incomprehensible which is called Cipher text. Plain text is either in the form that can be understood by a human being (document) or by a computer (executable code). Once it is transformed into Cipher text, neither human nor machine can perfectly process it until it is decrypted. This enables the transmission of confidential information over insecure channels without wrongful exposure. When data is stored on a computer it is protected by logical and physical access controls. When this equivalent sensitive information is sent over a network, the information is in much more vulnerable state. Naor and Shamir made known the new concept of Visual Cryptography in 1994, requiring no computation apart from human Visual System to decrypt. They recommended a basic (2,2) Visual Cryptography scheme where a secret image is split into 2 shares, expose the secret image through Share Stacking

Figure 1 a secret image that has to be sent is split into shares. When these two shares are stacked together and put into a Human Visual System the outcome image is revealed. In the visual secret sharing model, a secret picture must be shared among n participants. The picture is break into n shares so that if m transparencies (shares) are placed together the picture is visible[16]

(1.2) basic visual cryptography scheme
VC Strategy, the initial image is divided into two shares such that each pixel in the original image is replaced with a non-overlapping block of two either four sub-pixels. Anybody, having only one share can not get any information about the cover image. In the procedure of decryption, stacking of both the shares with each other can provide the information about the secret image. Encryption of a (2, 2)VC Strategy is shown in Figure 1
secret image into several shares so that only someone with all shares can decrypt the secret image by overlapping all shares together. It is image data hiding schemes based on error diffusion have the characteristics of visual cryptography with respect to driving of embedded data image. They embed secret image data into various halftone images without affecting their visceral qualities and the embedded data can be restored with apparently tremendous quality when the halftone images are overlaid without any extraordinary electronic calculation [6].

Fig 1.6 visual cryptography

(1.4) Visual cryptography techniques

(1.4.1) Multiple Secret Sharing Visual Cryptography Technique

two binary secret images are shared in two share picture A and B twin of which are binary image and is arbitrary. Shares are made such that the first secret can affirm the information as shown in basic model, that is, by superimposing two stake images, and the second share can be retrieve through rotating the first share i.e. share A by anticlockwise direction. A rotating angle 90° was seized. Wu and Chang refined the idea by programming share to be circles so that the stipulation to the rotating angle can be evacuated.

(1.4.2) The progressive visual cryptography

In this technique reconstruction of secret image is probabilistic and the stake image equal in size as Secret image size. The output of the secret image pixel is constructed using ‘OR’ operation practiced on the analogous pixel in share images. As the name probabilistic visual cryptography suggests, there is no absolute assurance on the correct reconstruction of the original pixel. It is distinctive from a traditional visual cryptography in that a defective reconstruction of pixel is possible. ‘Approximation’ of secret pixel is guaranteed in the classical technique. Here, approximation or we can say likeness means that a white (black) pixel can be, in some cases, replaced in the rebuild image by a set of sub pixels having a given set of whiteness (blackness). Since in probabilistic models the unknown pixel is inaccurately rebuild with some probability, the quality of the reconstructed images depends on how big is the probability of accurately rebuild the secret pixels.

(1.4.3) Random framework based visual cryptography technique

In this scheme magnitude of pixel is equal as original image pixel size. This means that retrieved secret image size and initial image size is same so it reduces the problem of pixel expansion. In this Method arbitrary grid R is explain as a two dimensional array of pixels. Each pixel is either transparent (white) or opaque (black) by a coin-flip strategy. The numbers
of clear pixels and opaque pixels are probabilistically same and the average opacity of a random grid is 50%.

(1.4.4) The Tagged Visual Cryptography Technique
It is an innovative type of visual cryptography in which extra tags is obscured into each develop share. By folding up each single share, the related tagged pattern is visually invented. Such supplementary tag patterns extremely supplement extra abilities of VC, such as upgraded message carried in a single share, fool-proof interface to manage the shares. However, reported (k, n) tagged visual cryptography proposed by Wang and Hsu still suffers from the fault such as pixel expansion.

A. Technique for Image Encryption using Digital Signatures
Technique to encrypt an image for secure image transmission. The digital signature of the initial image is added to the encoded version of the original image. Image encoding is done by using an revelant error control code, such as a Bose-Chaudhuri Hochquenghem (BCH) code. At the receiver end, after the decoding of the image, the digital signature can be used to double check the authenticity of the image.

B. Image Encryption using SCAN methodology which performs both lossless squeezing and encryption of binary and gray-scale images. The squeezing along with encryption techniques are based on SCAN patterns given by the SCAN procedure. The SCAN is a formal language-based two-dimensional spatial-accessing methodology which can efficiently specify and generate a vast range of scanning paths or space filling curves. The shortcoming of the algorithm is that it takes long time to encrypt[12].

(1.5) Security during transmission of images
In cheating avoidance in Visual Cryptography the following are the main modules and each module is explained below.

- Security & Login Module
- Encoding the Image
- Decoding the Image
- Verification of Images
- User Interface & Manual

Security & Login Module:
This caliber contract with ensuring that only authorized users can access to this application.A database with user-id and password is required to approve the User entry. The input user-id is approved for a minimum of four characters. The application accessible into the application screen on validation.

(1.6) Visual cryptography in internet voting for extended security
Internet voting system permits a voter to vote over the internet while providing accuracy and security. Internet voting scheme can be of two category-Poll-site and remote voting. Poll-site voting facilitates the voter to vote over the internet, at a voting poll. Remote voting permit the voter to vote from anywhere around the globe thus removing geographical restrictions.

(1.6.1) Two out of two visual cryptography schemes
In this category of Visual cryptography technology, the secret image is split into two shares. This is the uncomplicated kind of visual cryptography. The major utilization of this scheme is establish with IVS that uses 2 out of 2 Visual secret sharing schemes for authentication purpose. To reveal the initial image, two shares are required to be stacked together.

(1.6.2) k out of k visual cryptography scheme
In This form of visual cryptography scheme secret is split into k number of shares and for regeneration of the secret image, all k shares are desired. For example, in 6 out of 6 VC scheme, Secret is acknowledge only after stacking all the 6 shares, where k= 6. This scheme is not so famous because managing k number of shares is difficult task and it also increases time ramification. A voting system should be fair abundant for twain political parties and voters. There are some peculiar of voting system that are as follows-

- Authentication: Only authorized voters should be able to vote.
- Uniqueness: No voter should be able to vote more than one time.
- Accuracy: Voting systems should record the votes accurately.
- Integrity: Number of casted vote must not be alter.
- Verifiability: Possible to verify that votes are accurately counted in the final tally.
- Auditable: trustworthy and demonstrably credible election records.
- Reliability: Systems should task robustly, even in the face of numerous failures[1]

(1.7) Applications
Visual Cryptography technology can decode concealed images based purely on human Visual systems, without any aid from Cryptographic calculation. This good property gives birth to a wide range of encryption utilization. In this section, we will deal with how VCS is used in Applications such as E-Voting System, Financial documents and Copyright Protections.

1) Electronic Balloting System
These a days utter most of the Voting is managed with Computer Systems. These Voting Machines expected voters to faith them, with out giving testimony that they recorded each vote accurately. One way to solve this difficulty is to issue receipts to Voters to ensure them their votes are counted.

2) Encrypting financial documents
The VCS principle can also be practiced in transmitting confidential financial documents over Internet. VCRYPT is an example of this category of system being discover by Hawkes et al. VCRYPT can encode the original drawing document with a enumerate (k, n) VCS, then send each of the encoded n shares separately by Emails or FTP to the recipient[22].

LITERATURE SURVEY
The research work performed in this field by different researchers is presented as follows:

Linju P.S, Sophiya Mathews(2016), Visual cryptography is mechanism a of cryptography in which secret images are divided into multiple shares and are distributed to different entities. Each secret can be regenerated by superimposing these shares using different operations. Common traditional shortcoming of all existing methods is pixel expansion and noise at output. Another major issues that can occur in existing visual cryptography systems are deceiving between share holders and Share holders cheating owner. In order to conquered these limitations, sealing algorithm is used with two applications of VC such as MIVC and EVC. Here two secret images can be send at the equivalent time by converting them to halftone representations which in turn are partitioned as three shares in total[2].
Febin Baby, Arun R, Dr. Suvanam Sasidhar Babu(2016), Visual Cryptography is a unique kind of cryptographic technique in which the decryption can done by the human visual capability. In general, for some critical security issue the visual cryptography scheme is used, for example to analyze the distinction in human and machine. Security has become an inseparable issue as Information Technology is leading the world now. Cryptography in the study of mathematical procedure related aspects of information security such as confidentiality, data security, entity verification, but it is not only the means of providing information security, rather one of the scheme. Visual cryptography can be applied for copy right for images, access control to user images, visual verification and identification any kind images of images like(normal or digital). Visual cryptography is a new technique which gives information security which user simple algorithm unlike the complex, computationally demanding algorithms used in other schemes like traditional cryptography. Similarly some other applications also use the visual cryptography schemes like scanning and printing, etc. Hence the researchers developed many methods and procedure for the vc scheme. This paper is intended to study the different visual cryptography strategy and also to analysis the performance on the basis of expansion of pixel, number of undercover images, image format and type of share generated[3].

Asha Bhadran R(2015), With the advancement of digital media, it is becoming more common to find a method to protect the security of that media. An effective procedure for firmly transmitting images is found in the field of Visual Cryptography (VC). Visual cryptography scheme is a cryptographic technique that allow visual information (e.g. printed text, handwritten notes, and images etc) to be encrypted in such a manner that the decryption can be performed by the human visual system(HVS), without the subsidy of computers. The shares are protected because separately they reveal nothing about the secret image. The extraordinary characteristics of visual cryptography scheme is that one can visually decode the secret image by superimposing shares .By taking benefit of this property, third person can easily restore the secret image if shares are passing in sequence over the network. This paper demonstrate a visual cryptographic technique for color images in which the provoke shares are again encrypted. For this XOR operation is worn and this will grant double security for the secret document. Thus secret shares are not feasible in their actual form for any alteration by the adversaries who try to create bogus shares. The proposed scheme also uses the theory of halftoning[4].

Mr. Praveen Chouksey1, Mr.Reetesh Rai2(2015), Visual cryptography grant secured digital transmission which is used only for one time. The initial images can be reuse by using this scheme. It is easy and uncomplicated technique to execute the secret image for shadow images. The shadow images are the shrunken version of the primitive image, in which the secret image share is embedded. These are used to escort the data and secret images in the internet so that it is not accessed by any unauthorized persons. Visual cryptography break the image into secret shadow images. After this these shadow images are distributed in the original image. Improving of secret image is done by human visual system by piling all the shadow images[5].

Ms. Bhawna Shrivastava(2015), Image cryptography is appearing field of the research. There are various techniques has been established for cryptography. The many encryption techniques have been worn for obscure the visual information (pictures, text, etc.) in images. The fundamental concept of encryption is possibility of decryption by the human vision if the correct key image issued is termed as visual cryptography. In this paper, distinctive analysis has been discussed for Visual Cryptography[6].

Poonam (2015), Protection and Confidentiality is one of the most common aspects of information technology. The secure and effective protection of sensitive information or data is a primary matter in any scientific, military, medical and commercial systems. This is achieved using different techniques for different types of information or message. Visual cryptography is one such approach that secures visual information, which is a very secure and unique way to protect secrets. Visual cryptography is an encryption procedure which is used to cover encrypt information present in an image encrypted in such a way that the decryption can be executed by the human visual system, without the aid of computers. In this, images are distributed as shares that required to be superimposed to restore the hidden secret image. The intent of this paper is to study various visual cryptography (vc) system and research works done on the basis of pixel expansion, number of secret images and the merits and demerits of each[12].

Akshatha M M, Lokesh B, Nuthan A C(2014), As the advancement in the technology increases maintaining the security of visual information during its transaction has to be increased. Swift growth in the techniques for doing so is also increasing. Internet has become most commonly used media for transmission and hence text, voice, video, Images and many more are transmitted through Internet. These might include Military Secrets, economic Secrets and Information of individuals and therefore it has to be transmitted by safer means with upgrade security. In the process of Visual Cryptography a secret image is encrypted into shares which refuse to divulge information about the original secret image. In this paper, Chaotic Pseudo – Random Number generation, Zigzag Scan Pattern Method, process to reduce the degradation of the resultant image is proposed by an extension from gray to colour image. Pixel Index process is explain to improve the security for images. An integration of this procedure of Visual Cryptography with (n, k, p) gray image is also proposed[16].

Mounita Pramanik1, Kalpana Sharma(2014), Information Security has become an inseparable problem in the rapid growth of computer and communication technology. Data or information is vulnerable to various attacks. Although, cryptography system is used to protect data, still it suffers various problem viz., computational complexity, processing delay and more storage medium. Visual Cryptography (VC) is an emerging cryptographic scheme, which divide an image into different shares in its encryption process and the image can be decoded by stacking the shares with each other. Decryption process is not required any cryptography knowledge as it need the human visual system to recover the original image. Various visual cryptography schemes have been proposed so far. This paper reviews few VC schemes with its distinct characteristics[13].
Urvashi Yadav, Nisheeth Saxena (2014), Visual cryptography allows the data to be encrypted using an encoding scheme. It does not require a computer to decode. Two permeable images are used in Visual Cryptography. One image contains the secret information and the other image contains random pixels. It is impossible to acknowledge the secret information from one of the images as both transparent images are needed to retrieve the information. In this paper, author working on the security of visual cryptography. Author gave a new scheme termed as three level sharing. In this case, author renhance the security of an image by dividing into shares and then after sub shares. For this objective, stamping algorithm is used[15].

R. Yadagiri Rao (2013), An impressive and secure protection of sensitive information is the primary concerned in Communication systems or network storage systems. Never the less, it is also essential for any information process to ensure data is not being tampered with. Encryption methods are one of the prominent approaches to ensure the integrity and confidentiality of the protected information. However one of the censorsious vulnerabilities of encryption techniques is protecting the information from being disclose. To address these reliability complications, especially for large information content items such as secret images (satellite photos or medical images), an image secret sharing schemes (SSS) is a good alternative to remedy these types of vulnerabilities. With the swift advancement of network technology, multimedia information is transmitted over the Internet readily. While using secret images, security issues should betake into consideration because hackers may utilize weak link over communication network to abduct information that they want. To deal with the security problems of secret images, different image secret sharing method have been developed[22].

Sagar Kumar Nerella* Kamalendra Varma Gadi Raja Sekhar Chaganti (2012), Visual Cryptography is a advanced Cryptography technique which is used to secure the images. In Visual Cryptography the Image is partition into parts called shares and then they are distributed to the participants. The Decryption side just bundle the share images gets the image. The fundamental model developed only for the bi-level or binary images or monochrome images. Later it was progressive to suit for the Colour Images means Gray Images and RGB/CMY Images. For the RGB/CMY Images different procedure are establish based on the colour decomposition techniques. In this paper author discover a new way of operating colour visual cryptography using wavelet technique. Wavelet technique is used to convert the Colour Image to Gray Image. The essential quality of the Visual Cryptography is decryption doesn’t require any computer and it requires less computational power[24].

Jagdeep Verma, Dr. Vineeta Khemchandani (2012), The Visual cryptography scheme (VCS) is a protective method that encrypts a secret image by dividing it into shares. A extraordinary property of VCS is that one can visually decode the secret image by superimposing shares without computation. The project presents an approach for embedding visual cryptographically generated image shares in the host images to grant authentication for the VC shares and makes these secret shares imperceptible by embedding them into host images. The secret shares establish from VC encryption are watermarked into some host images using digital watermarking. Digital watermarking is used for granting the double security of image shares. The share is embedded into the host image in frequency realm using Discrete Cosine Transform (DCT). In frequency domain, the obtained marked image must be less distorted when compared to the primary image. Thus secret shares are not accessible for any alteration by the adversaries who try to create bogus shares. Every pixel of the binary VC share is imperceptible embedded into the individual block of the host image. The method of watermark eradication necessitates only the watermarked image and it does not need the original host image. The scheme grant more secure and meaningful secret shares that are robust against a number of attacks like blurring, sharpening, motion blurring etc[25].

3. PROBLEM FORMULATION AND OBJECTIVE

3.1 PROBLEM ANALYSIS
A technique for securing the visual content is “Visual Cryptography” and that visual content can be text, images etc. This security is provided with the help of encryption means that the message or an image is encoded in such a way that any unauthorized user(hacker) must not get access to its original meaning. The first issue was that the concept of visual cryptography was applicable only for binary images not for gray scale images.

The main concept used for this type of security of images is to divide an image into shares and distributing those shares to different participants. Stacking all those shares together is the solution to get an original image back but the main issue is that absence of any one of these shares makes it difficult to retrieve the original image back after decryption. Another issue is that sometimes while stacking the shares of an image together, original image quality is lost and that quality needs to be maintained. Size of reconstructed image should also be same as that of original image. Sometimes the encrypted data is meaningless that is another main issue concerned with the concept of visual cryptography. This is the detailed analysis of our problem.

3.2 PROBLEM STATEMENT
Here, we will discuss objectives of our proposed work. The main objectives that we are going to implement are:

3.2.1 To develop a (4, 4) visual cryptography scheme: This is the first objective of my proposed work. Firstly, the concept of (2, 2) visual cryptography technique was proposed but now we are extending this to (4, 4) visual cryptography which has not been implemented so far. In (2, 2) visual cryptography scheme, secret image is divided into two shares i.e share 1 and share 2. Both shares need to be stacked in order to reveal the original image. Original image will be recovered by stacking the two shares using bit OR operation.

3.2.2 To ensure more security to shares, the shares can be encrypted using DES algorithm: Now a days Security is the main issue related to stealing of secret information. So Dividing an image into shares and then stacking them together is not sufficient. There is need to adopt strong security approach that can ensure more security to the shares of an original image. That security can be ensured by using an algorithm and that algorithm is Data Encryption Standard (DES). Its proper name is Data Encryption Algorithm. The two fundamental building blocks of encryption are Substitution and Transposition. Data Encryption Standard is a complex combination of these two.
fundamental building blocks. The strength of this algorithm is derived from the repeated application of these two techniques (Substitution and Transposition) one on the top of the other and for a total of 16 cycles.

4.PROPOSED WORK
(4.1) PROPOSED WORK FOR VC
Presently the generated shares are meaningless i.e. the shares do not express any meaning. Meaningful shares can be generated by using the concept of cover image so that just by viewing the shares no one can guess that there is some secret data encrypted in that image. The shares can be encrypted using DES algorithm to ensure more security to shares so the present work can be improved by removing the unwanted colors from the decrypted image and extended to (n,n) cryptography scheme.

(4.2) SOFTWARE REQUIREMENTS
(4.2.1) MATLAB
MATLAB is a high-achievement language used for technical computing. It integrates computation, visualization, and programming in an effortless-to-use environment where complication and solutions are expressed in familiar mathematical notation. Typical practice includes:

- Math and computation
- Algorithm advancement
- Modelling, simulation, and prototyping
- Data test, exploration, and visualization
- Scientific and engineering graphics
- Application evolution, including Graphical User Interface building

MATLAB is communal system whose basic data element is an array that does not require dimensioning. This allows you to work out many technical computing obstacle, especially those with matrix and vector formulations, in a fraction of the time it would take to create a program in a scalar non interactive language such as C or FORTRAN. The name MATLAB sentiment for matrix laboratory. MATLAB was initially written to provide easy access to matrix software developed by the LINPACK and EISPACK projects, which is well organised and represent the state-of-the-art in software for matrix computation. MATLAB has emerged over a period of years with input from many users. In university environments, it is the standard instructional apparatus for introductory and advanced courses in mathematics, engineering, and science. In industry, MATLAB is the tool of exclusive choice for immense-productivity research, development, and analysis. MATLAB factor a family of application-specific solutions known as toolboxes. Very important to most users of MATLAB, toolboxes allow you to learn and employ specialized technology.

(4.2.1) THE MATLAB LANGUAGE
This is a high-level matrix/array language with curb flow statements, functions, data structures, input/output, and object-oriented programming features. It allows a pair "programming in the small" to briskly create quick and dirty throw-away programs, and "programming in the large" to build up effective large and complicated application programs.

MATLAB has several benefits over other methods or languages:

- Its elemental data element is the matrix. A simple integer is treated an matrix of one row and one column. A few mathematical procedures that work on arrays or matrices are built-in to the Mat lab.

MATLAB is communal system whose basic data element is an array that does not require dimensioning. This allows you to work out many technical computing obstacle, especially those with matrix and vector formulations, in a fraction of the time it would take to create a program in a scalar non interactive language such as C or FORTRAN. The name MATLAB sentiment for matrix laboratory. MATLAB was initially written to provide easy access to matrix software developed by the LINPACK and EISPACK projects, which is well organised and represent the state-of-the-art in software for matrix computation. MATLAB has emerged over a period of years with input from many users. In university environments, it is the standard instructional apparatus for introductory and advanced courses in mathematics, engineering, and science. In industry, MATLAB is the tool of exclusive choice for immense-productivity research, development, and analysis. MATLAB factor a family of application-specific solutions known as toolboxes. Very important to most users of MATLAB, toolboxes allow you to learn and employ specialized technology.

MATLAB is communal system whose basic data element is an array that does not require dimensioning. This allows you to work out many technical computing obstacle, especially those with matrix and vector formulations, in a fraction of the time it would take to create a program in a scalar non interactive language such as C or FORTRAN. The name MATLAB sentiment for matrix laboratory. MATLAB was initially written to provide easy access to matrix software developed by the LINPACK and EISPACK projects, which is well organised and represent the state-of-the-art in software for matrix computation. MATLAB has emerged over a period of years with input from many users. In university environments, it is the standard instructional apparatus for introductory and advanced courses in mathematics, engineering, and science. In industry, MATLAB is the tool of exclusive choice for immense-productivity research, development, and analysis. MATLAB factor a family of application-specific solutions known as toolboxes. Very important to most users of MATLAB, toolboxes allow you to learn and employ specialized technology.

MATLAB has several benefits over other methods or languages:

- Its elemental data element is the matrix. A simple integer is treated an matrix of one row and one column. A few mathematical procedures that work on arrays or matrices are built-in to the Mat lab.

MATLAB is communal system whose basic data element is an array that does not require dimensioning. This allows you to work out many technical computing obstacle, especially those with matrix and vector formulations, in a fraction of the time it would take to create a program in a scalar non interactive language such as C or FORTRAN. The name MATLAB sentiment for matrix laboratory. MATLAB was initially written to provide easy access to matrix software developed by the LINPACK and EISPACK projects, which is well organised and represent the state-of-the-art in software for matrix computation. MATLAB has emerged over a period of years with input from many users. In university environments, it is the standard instructional apparatus for introductory and advanced courses in mathematics, engineering, and science. In industry, MATLAB is the tool of exclusive choice for immense-productivity research, development, and analysis. MATLAB factor a family of application-specific solutions known as toolboxes. Very important to most users of MATLAB, toolboxes allow you to learn and employ specialized technology.

MATLAB has several benefits over other methods or languages:

- Its elemental data element is the matrix. A simple integer is treated an matrix of one row and one column. A few mathematical procedures that work on arrays or matrices are built-in to the Mat lab.

MATLAB is communal system whose basic data element is an array that does not require dimensioning. This allows you to work out many technical computing obstacle, especially those with matrix and vector formulations, in a fraction of the time it would take to create a program in a scalar non interactive language such as C or FORTRAN. The name MATLAB sentiment for matrix laboratory. MATLAB was initially written to provide easy access to matrix software developed by the LINPACK and EISPACK projects, which is well organised and represent the state-of-the-art in software for matrix computation. MATLAB has emerged over a period of years with input from many users. In university environments, it is the standard instructional apparatus for introductory and advanced courses in mathematics, engineering, and science. In industry, MATLAB is the tool of exclusive choice for immense-productivity research, development, and analysis. MATLAB factor a family of application-specific solutions known as toolboxes. Very important to most users of MATLAB, toolboxes allow you to learn and employ specialized technology.

MATLAB has several benefits over other methods or languages:

- Its elemental data element is the matrix. A simple integer is treated an matrix of one row and one column. A few mathematical procedures that work on arrays or matrices are built-in to the Mat lab.
the effect of change in plain text throughout the resulting cipher text and the basic tool for diffusion is Transposition. Basically, Substitution is represented by S-Boxes and Transposition is represented by P-Boxes. Data Encryption algorithm is an iterative algorithm that uses table lookups and simple bit operations. First of all, Input to the DES is arranged in the form of 64 bit blocks. We know that this algorithm operates on the blocks of data. So the 64 bit input is divided into two halves (Left Half and Right Half) each of 32 bits. Each half is scrambled independently, key is combined with one half and then the two halves are swapped. This is called 1 cycle and the process is repeated 16 times. The following are the steps of an algorithm along with its flowchart.

(4.4.1) EXPANSION PERMUTATION: The very first step of this algorithm is Expansion Permutation. The main intent behind expansion permutation is to make intermediate halves of the cipher text comparable in size to the key and provide a longer result that can later be compressed. In this, there is an expansion of right half from 32 to 48 bits. In this, order of the bits is permuted and also the certain bits are repeated.

![Flowchart of DES](image1)

(4.4.2) Key Transformation: Here the key length is of 64 bits but we will use only 56 bits as a key in our proposed algorithm by removing every 8th bit (8, 16, 24, ….,64). This is because these 8 bits are used as parity bits and no information is carried by these parity bits in the key. This process is called key transformation. There is a splitting of a key into two 28-bit halves at each step in the cycle. There is a left shifting of these two halves by a specified number of bits which are then pasted together again. Out of 56 bits, 48 bits are permuted to use as a key during this cycle. After key transformation, 48 bit key is combined with expanded right half by using an exclusive-or operation.

(4.4.3) S-BOXES: S-Boxes are used to perform substitution based on a table of 4 rows and 16 columns. It is a permuted choice function in which there is a replacement of 6 bits of data by 4 bits. There are 8 S-Boxes. Here, 48 bit input is divided into eight 6-bit blocks identified as B1, B2, B3, …., B8. S-Box Sj operates on block Bj. Suppose that block Bj is 6 bits i.e. b1, b2, b3, b4, b5, b6. Bits b1 and b6 having a decimal value from 0 to 3 form a two bit binary number and is equal to the value of row i.e. represented by r. Bits b2, b3, b4, b5 having a decimal value from 0 to 15 form a decimal number which is equal to the value of the column that is represented by c. 4.1.1.4 P-BOXES: All 32 bits of the result obtained after an S-Box Permutation are permuted by straight permutation. Here the bits will be moved to different positions and there will be 8 bits on each row. Basically, there are two types of permutations that are employed in this algorithm. One is Initial Permutation in which the 64 bits of each input block is reordered. Another is Final Permutation that is used at the conclusion of 16 substitution permutation rounds.

(4.4.4) COMPLETE DES: Now, all the different pieces are combined together to form complete DES. Firstly, 64 bit key is reduced to 56 bits. Then the initial permutation is carried on the 64 data bits. There are 16 cycles in which key is shifted and permuted. There is a transformation of half of the data block with the substitution and permutation functions and the result is combined with the remaining half of the data block.

(4.5) FACILITIES REQUIRED FOR PROPOSED WORK: Here, we require facilities for the following: 1. Generation of meaningful shares. 2. Encryption of those shares using AES. 3. (4.4) Visual Cryptography Scheme.

5. RESULTS AND DISCUSSION:
5.1 Various steps to obtained results
- Algorithm is implemented in MATLAB.
- Open the MATLAB.
- Go to the FILE option and click on the OPEN button and select the main program from the file.
- After that program will be open.
- Then click on RUN button to run the program.
- Select the COVER image from file that is to be used as shown below in figure (5.1)

![Cover Image from MATLAB Window](image2)

- Then select the MESSAGE image from file which is to be send as shown in figure (5.2)

![Message Image from MATLAB Window](image3)
Then provides the number of L.S.B BITS here, we are providing L.S.B as shown in figure(5.3)

Figure(5.3) LSB Bits In Matlab Window

After L.S.B is given it provide PSNR of message image to extracted image shown below in figure (5.4)

Figure(5.4) PSNR MESSAGE WINDOW

Then save the stenographic image in file of your choice.
Open the next program from file.
Run it again by clicking run button.
Select the stenographic image which is saved earlier as shown in figure(5.5)

Figure(5.5) SELECTED STEGNOGRAPHIC IMAGE

Then entry key of your choice here we have given key 345.

Figure(5.6) MATLAB COMMAND WINDOW

Again key is asked same key enter 345, shown below

Figure(5.7) MATLAB WINDOW FOR KEY MATCHING

After entering key result elapsed time is 2.97914 shown below figure(5.8)

Figure(5.8) MATLAB WINDOW AFTER MATCHING

Cover image: cover image is the image which is used cover or hide the message image so that hackers or unauthorized person cannot view.

figure(5.9) cover image
MESSAGE IMAGE: message image is image which has meaningful information that we want to send and this is to be hide by cover image as shown below in figure (5.10).

Fig (5.10) Message Image

Steganographic Image: Steganography as the hiding of an image within another so that the presence of the hidden image is indiscernible. The key concept behind steganographic image is that image to be transmitted is not detectable to casual eye.

Fig (5.11) Steganographic image

EXTRACTED IMAGE: extracted image is receive same as message image its shown below

Fig (5.12) Extracted image

Here graph shows the encoding and decoding of the original image. Here, we can observe that there is a variation of different parameters due to which different cipher text are produced for the same plain text. On the other hand, same decipher text is produced at the decryption end i.e. the same secret message will be retrieved after the decryption shown below in Graph (5.1).

Graph (5.1) A graph for cipher text, decipher text

Histograms are one of the most prevailing graphs used to display numeric data. Histograms are easy to understand and can instantly tell you a lot about your data. Her histograms of input image and final image is same there is no change but different from encrypted image as shown below.

Graph (5.13) Histogram for input & final image

6. CONCLUSION AND FUTURE SCOPE

Visual Cryptography is an exclusive encryption technique to hide information in images in such a manner that it can be decrypted by the human vision if the appropriate key image is used. Here we have implemented successful a (n, n) visual cryptography scheme meaningf ul shares can be generated by using the concept of cover image so that just by viewing the shares no one can guess that there is some secret data encrypted in that image. The shares can be encrypted using DES algorithm to ensure more security to shares result evaluated by help of histograms and des algorithm is performed on matlab.

Future Scope: The proposed system can be extended using lossless Image compression methodology. Compressed image has less redundancy than the original image, crypt analysis will be difficult.

7. ACKNOWLEDGMENTS

First of all, I would like to thank Almighty GOD and my Parents for providing me the strength and opportunity to carry out this work. Thanks to all those researchers who published articles and helped to understand about visual cryptography, who contributed in the development of increase in Security in Visual cryptography using DES.
8. REFERENCES


27. T. Hoang Ngan Le a, Chia-Chen Linb, Chin-Chen Chang c,d, Hoai Bac Lea, “A high quality and small shadow size visual secret sharing scheme based on hybrid strategy for grayscale images”, © 2011 Elsevier Inc. All rights reserved. oi:10.1016/j.dsp.2011.07.004.


