SECURE VISUAL CRYPTOGRAPHY SCHEME WITH MEANINGFUL SHARES

Jinu Mohan
Research Scholar, Bharathiar University, India
jinumohan@gmail.com

Rajesh R
Associate Professor, CHRIST (Deemed to be University), India
r.rajesh@christuniversity.in

Abstract - Visual cryptography is an outstanding design, which is also known as visual secret sharing. It used to encode a secret portrait into various pointless share images. Normally, item bossed on transparencies and decrypts as loading one or two or the entire share images by means of the human visual system. Suppose, if we encompass great sets of secret shares then the pointless shares are complicated to handle. In this paper, a meaningful secret sharing algorithm and a modified Signcryption algorithm is used to enhance the security of the Visual Cryptography encryption schemes. The foremost intend of the anticipated format is to extend consequential shares and similarly make sure the isolation on conveying the secret data. The anticipated process is executed in the functioning platform of MATLAB and the presentation results are investigated.

***Keywords*:** Visual Cryptography, Elliptic Curve Cryptography (ECC), Signcryption algorithm, Password based Authentication.

1. Introduction

Nowadays, the multimedia information is quickly and simply conveyed by internet in the quick expansion of network technology. Even the private information like military maps are also conveyed by the networks. Cryptography is the analysis of constructing symbols to protect the privacy and data reliability [1]. Visual cryptography is a cryptographic procedure which is used to permit visual information (pictures, text, etc) as encrypted and that the decryption is carried out by means of the human visual system, devoid of the computer support. Some of the VC benefits are key supervision, message suppression, approval, verification, recognition, and distraction. VC system is absolute safe and supply indestructible encryption. Suppose, if an unsystematic share contains unsystematic pixels, then it is observed as a one-time pad system [2]. VC offer quick decryption devoid of any compound calculation by the help of conventional cryptographic process like data encryption standard (DES) format and advanced encryption standard (AES) format.

Encryption procedure is used to create unsystematic shares devoid of the help of secret key. This procedure is also recognized as visual cryptography. Visual cryptography is a method, in which, the innovative secret image is encrypted as several secret shares [3]. The foremost advantage of this process is that the secret image is decrypted by the human visual system devoid of calculation. VC is a lossless procedure which encompasses two most important benefits (a) it supplies a completely safe method to defend secret messages (b) the human visual system (HVS) is used to recognize secret messages openly devoid of any calculation if recovering encrypted messages [4].

The encryption of visual data contains visual Information pixel synchronization and fault dissemination procedure for elevated eminence. Synchronization decoding includes the pixels through the secret images for the period of fault dissemination which distribute delightful to human visual system [5]. The noise produced by means of the predetermined pixels which is gentle through the adjacent pixels. It is a cryptographic format to accomplish visual secret sharing. Particularly, a group of informative images are also known as objective or secret images. It is divided as a group of shares or described as shadow images, which are documented in transparencies [6]. Each one distribution is not exposing several sections of secret dwell in objective images. Suppose, if one is competent to obtain a quantity of permissible shares related through the application's contact format and load them collectively, then the hidden secret disseminated in the middle of these shares which is revealed by means of examining the superposed image through our eyes.

A section augmenting visual secret sharing format is that the encoded innovative image is containing extra stage of secrets which is based on the shares in the decoding progression [7]. This possession of augmenting revelation of the quantity of secrets in an image develops the achievable request of VC format. The measurement of every created share in the procedure of RG is identical to the dimension of innovative secret image. The feature is based on superior possessions in VC format because it constructs the effectual storage for the engendered shares. This document is also containing the designing ANN-level augmentation [8]. VC format devoid of pixel development utilizing the conception of RG which contains the subsequent possessions: (1) every produced share contains the identical dimension among the innovative image; (2) the quantity and position of not exposed secrets are maintained secret on the loaded shares, and (3) the quantity of secrets exposed is comparative to the quantity of shares occupied in the decoding progression; and (4) the decoding progression is carry out by means of examining the well loaded shares with human eyes devoid of any calculation [9]

2. Literature Review

Ching-Nung Yang et al[10] have clarified a visual cryptography scheme (VCS). Here, the trader encodes the secret as n shade images. Each one pixel of the secret image was ‘‘expanded’’ as m sub-pixels in each one distribution. In a (k,n)-VCS, the secret is visually renovated if k or additional distributions are offered. The renovation progression utilizes the individual visual system and no calculations are necessary. To resolve the pixel development difficulty of VCSs, probabilistic VCSs are openly rehabilitated from VCSs through no pixel development. An additional renowned secret image distribution format, random grid (RG) is as well supplied by means of these original stacking-to-see possessions. Contrast by means of VCS, the majority attractive advantage of RG is that there was no pixel development. The probabilistic VCS devoid of pixel development, to analysis the production and presentation of RG it encompasses two foremost consequences: (i) They illustrate that each one segment of the distribution production progression in the entire obtainable (2,2)-RG, (2,n)-RG, (n, n)-RG, (k,n)-RG, incremental RG is recorded to an equivalent step in PVCSs, and their outline images among PVCS and RG are completely identical and the renovated images are identical, as well comprise our (2,n) RG. (ii) Since the eminence of renovated image, pixel development, predictable area size, and image category to be measured for estimating PVCSs and RGs, they indicate that RG and PVCS contain no dissimilarity except the expressions. Additionally, RGs is a division of PVCSs.

Dao-Shun Wang et al[11] have explicated a visual cryptography scheme (VCS). It is an encryption procedure that exploits the human visual system in improving a secret image and it does not necessitate several compound computations. On the other hand, the dissimilarity of the renovated image is somewhat small. A quantity of reversing-related VCSs (or VCSs among repealing) (RVCS) is employed for binary secret images, permitting applicant to carry out a repealing function on distributions (or shadows). This repealing function is simply executed by means of existing copy machines. Several obtainable conventional VCS format devoid of repealing (nRVCS) is unlimited to RVCS among the identical pixel development for binary image, and the RVCS is accomplish ultimate dissimilarity, considerably advanced than the equivalent nRVCS. In the function of grayscale VCS, the dissimilarity is greatly lesser than the binary conditions. So, it is extra attractive to develop the dissimilarity in the grayscale image renovation. Though, if the grayscale images are implicated, then one obtains benefit of this repealing function so effortlessly. Numerous obtainable grayscale nRVCS is not openly unlimited to RVCS. They initially provide an innovative grayscale nRVCS among least pixel development and offer a most favorable-dissimilarity grayscale RVCS (GRVCS) through source matrices of ideal black nRVCS. Furthermore, they employ a most favorable GRVCS even if the source matrices are not completely black.

Xuehu Yan et al[12] have depicted a significant distribution in visual cryptography (VC).It is a preferred attribute as it augments the effectiveness of organization and diminish the misgiving of secret image encryptions. Even though the conventional user-friendly random grid (RG)-related VC is construct consequential distribution, through the benefit of no pixel development and no require for codebook plan, existing user-friendly RG-related VCs be unsuccessful to maintain the common (k,n) threshold and the corresponding distributions are necessary. A widespread RG-related VC among consequential distributions is exploited. Moreover, take over the superior attribute of no pixel development and no codebook design, format is maintain (k,n) threshold and supply adaptive visual eminence, at the expenditure of somewhat diminishing visual eminence of distributed images.

Xiaotian Wu et al[13] have clarified a tagged visual cryptography (TVC).It is a kind of visual cryptography (VC) in which supplementary tags is obscured by the engendered distribution. From solitary distribution, the related tagged model is visually exposed. These supplementary tag models are deeply augmenting additional capability of VC like enlarged message approved in a solitary distribution, accessible boundary to handle the distributions, and/or confirmation for authenticating reliability between those distributions collaborating in a decryption illustration. On the other hand, statement (k, n) TVC exploited by means of Wang and Hsu still experience from the faults like pixel development, code book necessary in the encoding segment and small image eminence. It has resolved the pixel development and code book required difficulties. Additionally, corrupt movement is prohibited by means of the anticipated algorithm. Advanced visual eminence of the improved secret image and renovated tag image is offered by the hypothetical investigation.

Ming-Shi Wang et al[14] have declared an official document defense format that unite the discrete wavelet transform (DWT) and the singular value decomposition (SVD). In place of altering the innovative host image to obscure a secret image, the employed format initially removes the image attributes from the congregation image by means of implementing the DWT and the SVD. The removed attributes are categorized as two groups by means of utilizing the k-means clustering procedure, and a master distribution is engendering by means of the clustering consequence. At last, the master distribution is employed collectively through a secret image to create an ownership distribution by a two-out-of-two visual cryptography (VC) procedure. Suppose, if the legal possession desires to be resolute, then the secret image for possession recognition is exposed by means of loading the master distribution and the possession distribution.

Paulius Palevicius et al [15] have declared a computer engendered hologram. It is frequently demoralized to execute visual encryption format. The incorporation of active visual cryptography (a visual procedure derived from the interaction of visual cryptography and time-averaging geometric moiré) is achieved through Gerchberg–Saxton algorithm. A stochastic is employed to implant the secret as a solitary cover image. The secret is visually decoded by means of uncovered eye if the amplitude of harmonic oscillations communicates to an exactly preselected value. The visual image encryption format is derived from computer engendered holography, visual time-averaging moiré and morality of active visual cryptography. Active visual cryptography is employed for the preliminary encryption of the secret image and the ultimate decryption. Segment data of the encrypted image is calculated by means of Gerchberg–Saxton algorithm. The visual image is decrypted by the computationally renovated area of amplitudes.

3. Problem Formulation

Visual secret sharing is a familiar format which is also known as visual cryptography. It encrypts a secret image into numerous pointless share images. Normally, it embossed on transparencies and decrypts as loading one or two or the entire share images by means of the human visual system. In recent times, several research document are anticipated about the visual secret sharing and its applications. Regrettably, the corrupt assaults like malicious contributors have counterfeit a false share image. In 2006, a few corrupt avoidance formats are anticipated but it also contains some difficulties: (1) preserving additional distribution images which are used to validate the reliability of a share image proceeding to loading, (2) establishing additional pixel development, and (3) providing unclear corrupt recognition. On the other hand, pointless distribution and pixel development are containing confront in obtainable XOR-related VC. Additionally, validation is the basic protection which is opposition to unlawful contact to a calculating device and additional responsive online functions. The validation in the course of a solitary feature is not consistent to supply sufficient defense of devices and functions. Therefore, multi-factor validation is a feasible choice to make possible constant defense of computing devices and supplementary serious online services from unlawful contact. Numerous validation method among unstable level of exactness and portability areaccessible for dissimilar kind of computing devices. The numerous obtainable and recognized multi-factor validation policies are exploiting to augment the protection of diverse functions. On the other hand, the requirement of explanation and the above mentioned difficulties motivated me to perform this research.

4. Proposed Secure Visual Cryptography Technique

This document is used to establish a safe visual secret distribution process along with password validation to ensure the protection of the Visual Cryptography scheme. Additionally, the anticipated Visual Cryptography format is premeditated to resolve the short image eminence and arrangement troubles in VC system. At this point, the innovative image is transformed into a quantity of significant shares. Therefore, it used to resolve the problem of fundamental visual secret sharing process which ensuing pointless shares. Additionally, a customized Signcryption algorithm is established to invent the privacy of secret image. The customized Signcryption algorithm utilizes Elliptic Curve Cryptography (ECC) process for engendering the confidential and non-confidential keys for the dispatcher and recipient. Additionally, password related validation format is engaged for the period of Un-Signcryption of the secret shares. Suppose, if the consumer go into the mistaken amalgamation of password/username for a limit of 3 times in validation, then the system is premeditated to be concluded. At last, the legitimate recipient is recovering the innovative secret image through carrying out the Ex-OR function on the secret shares.

The Block Diagram of proposed secure VC scheme with meaningful shares is depicted in the below Fig. 1

4.1 *Meaningful Secret Sharing Algorithm*

Pointless distribution and pixel expansion are considered as the foremost confront in obtainable XOR-related Visual Cryptography procedure. At this point, the fundamental algorithm for constructing a (n, n) XOR-related VC format is somewhat distorted to construct the consequential distribution. The anticipated consequential secret distribution algorithm develops the portrait eminence and ensures from the pixel expansion problem. Afterward, the consequential distributions are encrypted for defense intention.

Step 1: Matrix formation:

The (*n*, *n*) XOR-related VC format is created by means of engendering a $2^s \times s$ matrix, where ' S ' is the quantity of distribution required to be formed.

$$Y_S(x, 1: s) = de\ to\ bi(x - 1, s) \quad (1)$$

Where, x is $< 2^s$ and $de\ to\ bi$ denotes the decimal to binary conversion. The resultant matrix, Y_s includes the binary codes from 0 to $2^s - 1$. $2^s - 1$.

Step 2: Extract odd/even Matrices:

Nowadays, the consequential matrix is divided as odd and even matrices Y_s^{odd} and Y_s^{even}, because the odd and even sub-matrices are encompassing several significant possessions in the EX-OR consequence, if some row vector of indistinguishable possibility is preferred to load the created distribution.

The odd and even matrices of Y_s^{odd} and Y_s^{even} are acquired from the hamming loads of the row vector. Hamming load is indicating the quantity of 1's in the row vector. The odd matrix is the collection of row vector of matrix, $Y_s(x,1:s)$ whose hamming load is odd value. Similarly, the even matrix is the collection of row vector of matrix, $Y_s(x,1:s)$ whose hamming load is even value.

Step 3: Random Bit Generation:

For filling each pixel of the secret shares, a random bit generation step is followed, which is given as,

$$b = \begin{cases} 1, \text{with probability } \delta \\ 0, \text{with probability } (1-\delta) \end{cases} \quad (2)$$

Where, δ is a possibility value whose value is preferred among [0-1]. According to the unsystematic bit value, two dissimilar events are used to fill up the pixels of formed distribution. The eminence of secret image is enhanced for the period of the recovery progression for exacting values of δ.

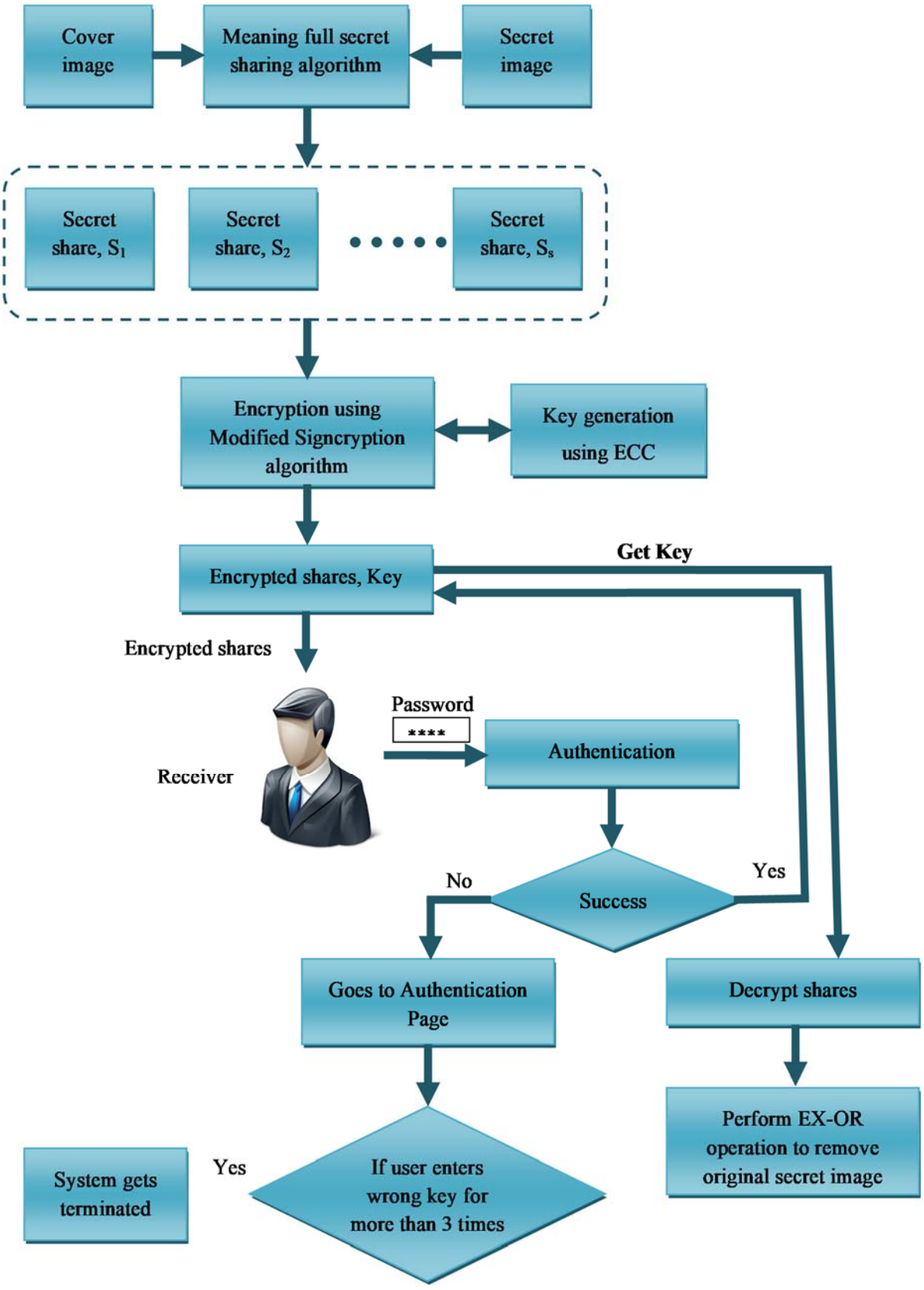

Fig. 1. Block Diagram of proposed secure VC scheme with meaningful shares

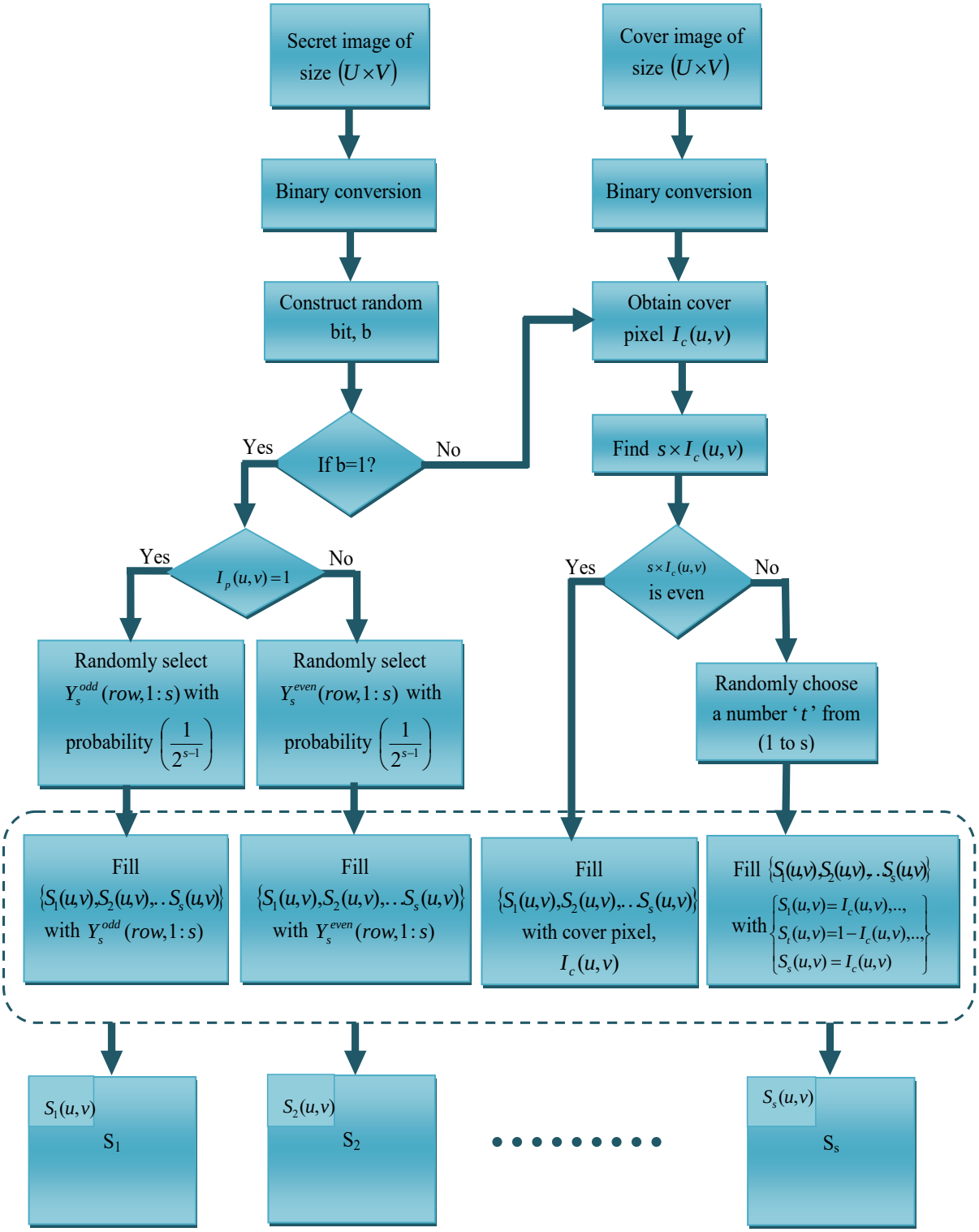

Fig. 2. Meaningful Secret Sharing Algorithm

Step 4: Share Creation:

Suppose, if the unsystematic bit is 1, then the secret distributions are overflowing through the row vectors of matrix, (Y_s^{even} / Y_s^{odd}) which is derived from the secret pixel value.

Moreover, if the unsystematic bit is 0, then the secret distributions are overflowing by the cover pixel values, in order to expand the consequential distribution.

Case 1: $b=1; I_p(u,v)=0;$

Suppose, if unsystematic bit is 1 then the secret pixel is 0. The secret distribution $\{S_1(u,v),\ S_2(u,v),\ldots\ S_s(u,v)\}$ is overflowing by the values from the row vector of even matrix ($Y_s^{even}(row,1:s)$), that is preferred erratically through indistinguishable possibility of $\left(\frac{1}{2^{s-1}}\right)$.

Case 2: $b=1; I_p(u,v)=1;$

Suppose, if unsystematic bit is 1 and then the secret pixel is as well 1, the secret distribution pixels $\{S_1(u,v),\ S_2(u,v),\ldots\ S_s(u,v)\}$ are overflowing by the values from the row vector of odd matrix ($Y_s^{odd}(row,1:s)$), that is preferred erratically through indistinguishable possibility of $\left(\frac{1}{2^{s-1}}\right)$.

Case 3: $b=0; I_p(u,v)=0;$

Suppose, if unsystematic bit is 0 and then the secret pixel is 0, the secret distribution pixels $\{S_1(u,v),\ S_2(u,v),\ldots\ S_s(u,v)\}$ are reinstated by means of the cover pixel $I_c(u,v)$.

Case 4: $b=0; I_p(u,v)=1;$

Suppose, if the unsystematic bit and the secret pixel are 1, then the quantity of distribution essential is developed by means of the cover pixel value, which is specified as, $f=s\times I_c(u,v)$.

Case 4(a): $b=0; I_p(u,v)=1;\ f=s\times I_c(u,v)$ is even;

Suppose, if $f=s\times I_c(u,v)$ is even, the entire secret distribution pixels $\{S_1(u,v),S_2(u,v),\ldots S_s(u,v)\}$ are overflowing by means of the cover pixels.

Case 4(b): $b=0; I_p(u,v)=1;\ f=s\times I_c(u,v)$ is odd;

Suppose if $f=s\times I_c(u,v)$ is odd, a secret distribution 't' is preferred from $(1\ to\ s)$ through possibility $\left(\frac{1}{s}\right)$ and reinstated by $(1-I_c(u,v))$. Though, residual distributions are overflowing by means of the cover pixels.

The proposed meaningful secret sharing algorithm is given in the below Algorithm_1.

Algorithm_1:Meaningful Secret Sharing Algorithm.

Input: Cover image - I_c of size $(U\times V)$; Secret Image - I_p of size $(U\times V)$; Probability - δ Output: $s=\{S_1,S_2,\ldots S_s\}$ number of meaningful shares each of size $(U\times V)$

// Matrix formation, Y_s of size ($2^s\times s$) for 's' number of shares required
For $x=1; x\le 2^s; x=x+1$
Do
{
$Y_s(x,1:s)=de\ to\ bi(x-1,s)$
}
End For
// Split Matrix Y_s into odd and even matrices (Y_s^{odd} and Y_s^{even})
For each $Y_s(row,1:s)$
Find Hamming weight, w_H
If ($w_H=odd$)
{
Add row vector $Y_s(row,1:s)$ to Y_s^{odd}

}
Else If($w_H = even$)
{
Add row vector $Y_s(row,1:s)$ to Y_s^{even}
}
End If
// Random Bit Construction, b
$b = \begin{cases} 1, \text{with probability } \delta \\ 0, \text{with probability } (1-\delta) \end{cases}$; where, δ is chosen randomly between $(0 \text{ to } 1)$
// Creating Secret shares
If ($b = 1$)
{
If ($I_p(u,v) = 0$)
{
Randomly choose row vector $Y_s^{even}(row,1:s)$ with probability $\left(\frac{1}{2^{s-1}}\right)$
Fill the shares $\{S_1(u,v), S_2(u,v), \ldots S_s(u,v)\}$ with $Y_s^{even}(row,1:s)$
}
Else If ($I_p(u,v) = 1$)
{
Randomly choose row vector $Y_s^{odd}(row,1:s)$ with probability $\left(\frac{1}{2^{s-1}}\right)$
Fill the shares $\{S_1(u,v), S_2(u,v), \ldots S_s(u,v)\}$ with $Y_s^{odd}(row,1:s)$
}
End If
Else If ($b = 0$)
{
Compute $f = s \times I_c(u,v)$
If(f is 'even')
{
$S_1(u,v) = I_c(u,v)$;
$S_2(u,v) = I_c(u,v)$;
…
$S_s(u,v) = I_c(u,v)$;
}
Else If (f is 'odd')
{
Randomly choose a number 'n' with probability $\left(\frac{1}{s}\right)$ from '$(1 \text{ to } s)$'
$S_1(u,v) = I_c(u,v)$;
…
$S_n(u,v) = 1 - I_c(u,v)$;
…
$S_s(u,v) = I_c(u,v)$;
}
End If
}
End If

Once when the meaningful shares are created, the secret shares are encrypted using modified Signcryption algorithm for privacy purposes.

4.2 *Signcryption Algorithm for encrypting Secret Shares*

In public key cryptography, Signcryption is an innovative model that simultaneously accomplishes the task of digital signature and public key encryption in a sensibly solitary step through an expenditure which is significantly minor than the expenditure of conventional signature and encryption methods. In Signcryption algorithm, the dispatcher is employing the recipient public key to signcrypt a message. Suppose, if the sender needs to transmit a Signcrypted text to a quantity of recipient then it encompasses a shortcoming; because, it requires to signcrypt the message through deliberate recipient public keys and send them independently to everyone. This method is unnecessary in expressions of bandwidth utilization and computational resource convention. This is resolved by means of the invention of cluster keys among the dispatcher and the recipient. Though, it used to develop the Signcryption algorithm and to make sure the isolation. At this point we utilize the customized signcryption algorithm to encrypt the secret distribution.

The anticipated customized signcryption algorithm encompasses four significant segments such as key production segment (using ECC), signcryption segment, Password related Authentication and Unsigncryption segment. In key production segment, private and public key for the dispatcher and recipient are engendered through Elliptic Curve Cryptography process. The foremost benefit is that it contains diminutive key size. Afterward it will depart to the signcryption segment, in which, the engendered distributions are encrypted by the aid of dispatcher private key and recipient public key. At last, the Unsigncryption is completed to recover the encrypted distribution; where the encrypted distributions are decrypted by the information specified from the dispatcher.

4.2.1. *Key Generation using ECC*

In this process, the key production is prepared by means of Elliptic Curve Cryptography (ECC) process for to construct the private and public keys of dispatcher and recipient. Elliptic Curve Cryptography (ECC) is recognizable like public key cryptography. Normally, it encompasses a couple of keys like a public key and a private key. A group of proceedings associated through the keys to terminate the cryptographic function. The noteworthy advantage of ECC is the diminutive key size. The tasks of elliptic curve cryptography are prepared by two fixed areas such as Prime region and Binary region. The suitable region is preferred for cryptographic function through finitely enormous quantity of position. The prime region function is used to choose a prime number. At this point, prime region function is made to choose the keys from a great choice of prime numbers, $[1,\cdots,n-1]$. According to the prime region function, we obtain the private and public key for mutually the dispatcher and recipient from a great choice of prime numbers, $[1,\cdots,n-1]$.

Let the Sender has the key pair, (k_{pvt}^{S}, k_{pub}^{S})

Where, k_{pvt}^{S} – Sender's private key

k_{pub}^{S} – Sender's public key

And the Receiver has the key pair is (k_{pvt}^{R}, k_{pub}^{R})

Where, k_{pvt}^{Rx} - Receiver's private key

k_{pub}^{Rx} - Receiver's public key

4.2.2 *Signcryption Phase*

Signcryption is a public-key primitive which is simultaneously implementing the task of digital signature and encryption. For the period of this segment, every secret distribution S_s is Signcrypted independently, which is derived from diverse couple of private and public of the dispatcher and recipient from the key production segment. Primarily, the dispatcher signcrypts the message S_1 and afterward the outstanding distributions, $\{S_2,\ldots S_s\}$ are signcrypted.

Steps involved in Signcrypting every secret share:

- An unsystematic value (*R*) is engendering from a great choice of values, $[1,\cdots,m-1]$ which is derived from dispatcher preference. Where, $[1,\cdots,m-1]$ is the series of prime feature of $[1,\cdots,n-1]$.
- According to the recipient public key k_{pub}^{Rx} and the indiscriminately engendered value (*R*), the one way hash task is calculated, in order that 128 bit value is engendered, which is specified as,

$H = hash\ (k_{pub}^{Rx} R \bmod n)$

- At this time, the dispatcher has to divide the 128 bit value (*H*), into two 64 bit values which is specified as, (H_1, H_2).
- Subsequently, the initial secret distribution S_1 is encrypted by means of a private key encryption format (K_{Enc}) among key H_1. For the period of encryption, a cipher text (*E*) is engendered, which is specified as,

  $E = K_{Enc} H_1(S_1)$
- Afterward, the dispatcher utilizes the key H_2 in the one-way key hash task, H to obtain a hash of the secret message S_1. The one-way key hash task $\hat{H}$ gives the consequencesof 128-bit hash, which is specified as,

  $\hat{H} = hash\left(key\ H_2, S_1\right)$
- At last, the restriction (*F*) is calculated by the dispatcher private key k_{pvt}^{S} which is engendered from the key invention segment, the engendered unsystematic value (*R*), great prime feature, *m* and the value of *H*. The limitation *F* is specified as,

  $$F = \frac{R}{(\hat{H} + k_{pvt}^{S}) \bmod m}$$
- Output: Three distinct values *E, H* and *F*

Three unrelated values of E , $\hat{H}$ and F are engendered for the period of Signcryption. Currently the dispatcher will send the secret distribution steadily to the recipient by means of sending the engendered three values (E , $\hat{H}$ and *F*). In the same way, the entire outstanding secret distributions are signcrypted by means of dispatcher private key and the recipient public key.

4.2.3 *Password based Authentication and Automatic Shutdown*

In this segment, the Password related Authentication is implemented on earlier than entering to the unsigncryption segment. The anticipated system is premeditated as that if the recipient enters the accurate password, then he will obtain the values of E , $\hat{H}$ and F from the Signcryption segment. The password is appearing in the structure of numbers or characters. At this point, we utilized arithmetical password that is preferred among the choice of 0 to 10. Suppose, if the recipient enters the incorrect password more than three times, then the system is concluded, and no function is carried out.

4.2.4 *Unsigncryption Phase*

Unsigncryption segment is take place at the recipient part for to recover the innovative secret distribution from the signcrypted message. Suppose, if the validation is success, then the recipient obtains the three unrelated values of *E, H* and *F* which is necessary for unsigncrypting the secret distribution.

Steps involved in Unsigncrypting the secret shares

- Get the three dissimilar values, E, $\hat{H}$ and from the sender
- Sender employ the values of *H, F* receiver's private key k_{pvt}^{Rx} , sender public key k_{pub}^{S} and *n* and *b* to calculate a hash which would result a 128 bit value.

  $H = hash\ ((k_{pub}^{S} * b^{\hat{H}})^{F} \times k_{pvt}^{Rx} \bmod n)$

  Where, *b* is the integer of order $m \bmod n$ chosen randomly from the range $[1, \cdots, n-1]$
- Next the 128 bit output is split into two 64 bit halves which would present the key pair of (H_1, H_2).
- Receiver then employs the key H_1 to decrypt the cipher text *E*, which will offer the message S_1; which can be represented as,

  $S_1 = K_{De} H_1(E)$
- Acknowledge S_1 as the valid message if one way keyed hash function on S_1 using the key H_1, $hash\left(key\ H_2, S_1\right) = \hat{H}$

Suppose, if the initial distribution is unsigncrypted, then the identical progression is take place for the outstanding distributions. Afterward, the recipient processes the EX-OR for recovered secret distributions to remove the secret data.

5. Results and Discussion

This section explained about the result and discussion of the anticipated protected Meaningful Visual Cryptography procedure with customized Signcryption algorithm. The anticipated algorithm is implemented by means of MATLAB software and the testing is carried out through a system containing 4 GB RAM and 2.10 GHz Intel i-3 processor.

The normal 'Lena.JPG' is observed by cover image for examination. At this point, we have obtained the 'twitter-logo' like the secret image. This enhanced secret image data is initially entrenched as the innovative image by means of the anticipated visual cryptography format to generate a group of consequential secret distribution. The investigational consequences for the anticipated protected VC format are distinguished by means of diverse image eminence limitations beneath diverse limitation.

The cover image, 'Lena.JPG' and the secret image 'twitter-logo' are given in the below Fig. 3.

(a) (b)

Fig. 3: (a) cover image; (b) secret image

5.1 *Graphical User Interface (GUI)*

The GUI of the suggested approach is given as,

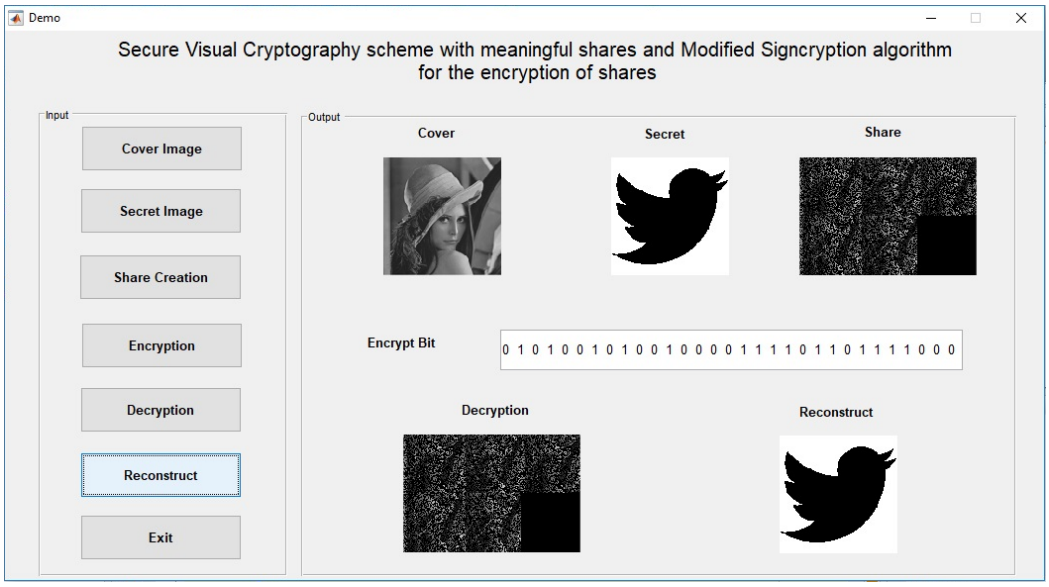

Fig. 4. GUI of proposed VC scheme

In Fig. 5, the Password Authentication Phase of the proposed VC scheme is given.

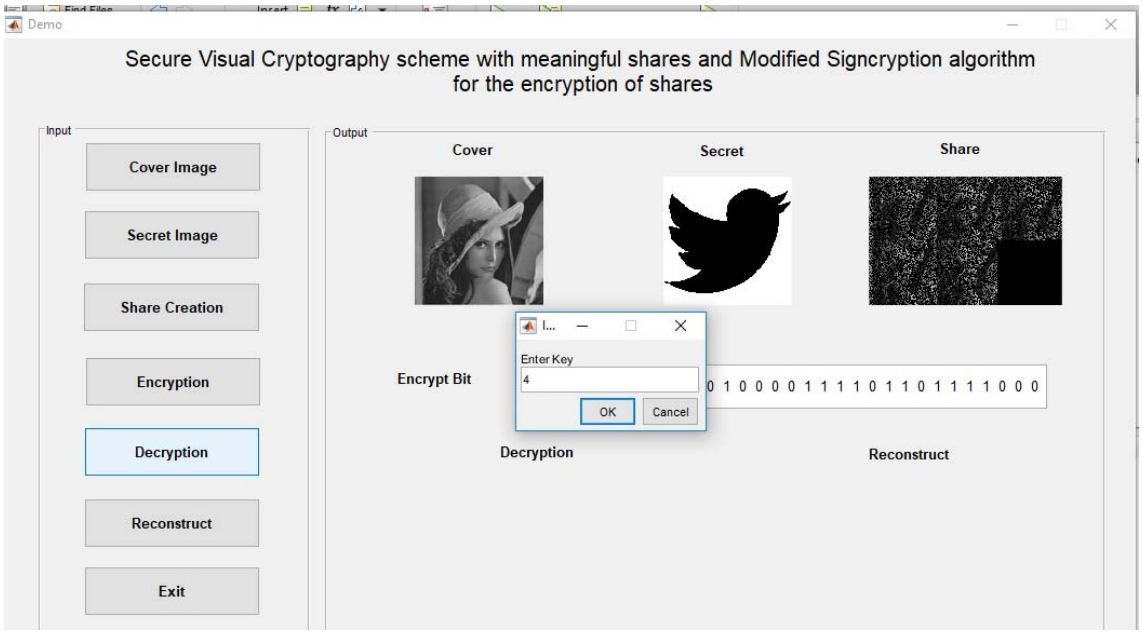

Fig.5 GUI of proposed VC scheme (Password Authentication Phase)

Moreover, the GUI showing the Rejection of Authentication on entering wrong password is given in the below Fig. 6.

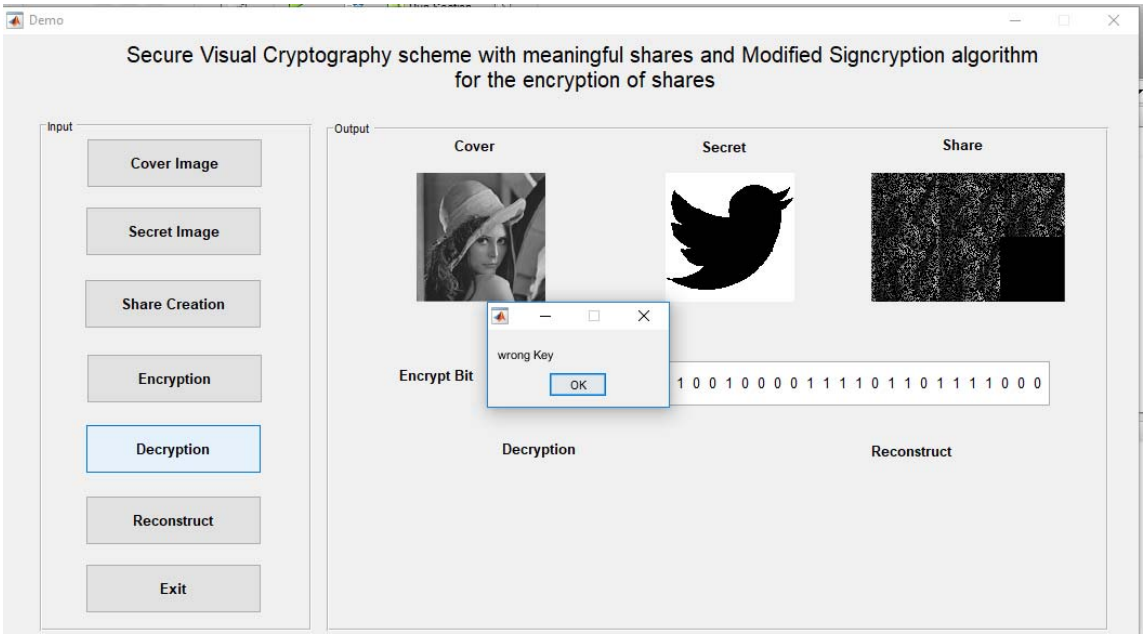

Fig. 6. GUI of proposed VC scheme (Rejection of Authentication on entering wrong password)

5.2. *Quality Analysis Parameters*

The presentation of the anticipated VC format is considered by means of basically computing the eminence of the innovative and the recovered images. The measures like Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Correlation Coefficient (CC) procedures are used to analyze among the innovative and the removed secret distributions for examining the presentation of embedding. Additionally, NC measure is calculated to estimate the eminence of removed and innovative secret image. In our anticipated VC format, the entire eminence metrics are estimated by means of unreliable delta value (i.e. a random value between0 to 1), which is employed for the period of the formation of secret distribution.

The mathematical representation of some of the undertaken measures are given as,

- **Mean Square Error (MSE):**

Mean Square Error is the squared dissimilarity among the cover image and the stego-image. Normally, the MSE is specified as,

$$mse = \frac{1}{UV}\sum_{u=0}^{U-1}\sum_{v=0}^{V-1}\left[I_c(u,v) - S_s(u,v)\right]^2 ; \quad (3)$$

Where, $I_c(u,v)$ and $S_s(u,v)$ are the cover image and created secret shares. And, $S_s(u,v) = \{S_1(u,v), S_2(u,v), \ldots S_s(u,v)\}$ represents the created shares.

- **Peak Signal to Noise Ratio (PSNR):**

Peak Signal to Noise Ratio is the peak fault in cover image and stego-image. The Peak Signal to Noise Ratio (PSNR) is generally exploited to compute the eminence of the watermarked image. In the superior PSNR value, the eminence image is improved. At the same time as, the lesser value of PSNR authorize the deprived eminence image.

$$psnr = 10\log_{10}\left(\frac{255^2}{mse}\right) \quad (4)$$

- **Normalized Correlation (NC):**

The dissimilarity among the innovative and the removed secret image is controlled by means of Normalized Correlation (NC), which is relating the arithmetical analysis of effectiveness presentation. Normalized Correlation (NC) is specified as,

$$nc(u,v) = \frac{\sum_{u=0}^{U-1}\sum_{v=0}^{V-1} I_p(p,q)I_p{}^*(u,v)}{\sum_{u=0}^{U-1}\sum_{v=0}^{V-1}\left[I_p(u,v)^2\right]} \quad (5)$$

The possible values of the normalized correlation output will be in the range of [0, 1]. Better correlation creates the value closer to 1.

5.3 *Performance Analysis*

The presentation evaluation of the anticipated protected VC format is exposed in this segment. At this point, the presentation is examined at each phase of the anticipated VC procedure.

I. *Performance Analysis of proposed VC scheme-based Embedding*

At this point, the presentation of embedding phase is estimated. The assessment is prepared by means of the image eminence evaluation of the innovative cover image and the generated distributions. The MSE, PSNR and Correlation Coefficient values accomplished are specified in the beneath tables 1 to 3.

Table 1 MSE between cover image and created shares

MSE					
Delta	**0.6**	**0.7**	**0.8**	**0.9**	**1**
Share 1	0.25411	0.258568	0.26071	0.260212	0.258294
Share 2	0.26005	0.255981	0.26183	0.257743	0.259473
Share 3	0.25718	0.258009	0.258363	0.256726	0.25861
Share 4	0.25752	0.258122	0.257635	0.257238	0.25927
Share 5	0.25718	0.258009	0.26183	0.257238	0.25861
Average	**0.2572**	0.25774	0.26007	0.25783	0.25885

In Table 1, it is obvious that the MSE is nearly identical for the entire distributions (i.e. between 0.25 to 0.26). Furthermore, the standard MSE is 0.25721 if the delta value equals 0.6. This illustrates that, if the delta is 0.6, then the dissimilarity among the cover image and the generated distribution is small.

Table 2 PSNR between cover image and created shares

PSNR					
Delta	0.6	0.7	0.8	0.9	1
Share 1	54.0806	54.00505	53.96923	53.97753	54.00966
Share 2	53.9802	54.04872	53.95061	54.01894	53.98988
Share 3	54.0285	54.01445	54.0085	54.0361	54.00435
Share 4	54.0227	54.01255	54.02075	54.02745	53.99328
Share 5	54.0285	54.01445	53.95061	54.02745	54.00435
Average	54.0281	54.0190	53.9799	54.0175	54.0003

In Table 2, it is distinguished that the entire values of the PSNR metric is as well roughly the collection of 53.

Table 3 Correlation Coefficient between cover image and created shares

Correlation Coefficient					
Delta	**0.6**	**0.7**	**0.8**	**0.9**	**1**
Share 1	0.232993	0.224126	0.231174	0.242193	0.242193
Share 2	0.238123	0.226918	0.223193	0.241479	0.241479
Share 3	0.210547	0.232114	0.21983	0.228233	0.228233
Share 4	0.211693	0.232744	0.218787	0.231396	0.231396
Share 5	0.21983	0.232993	0.241479	0.224126	0.211693
Average	0.22264	0.229779	0.226893	0.233485	0.2309989

The Table 3 explains about the values of Correlation Coefficient among cover image and generated distributions. It is observed from the above table; the standard CC is elevated for the distributions if the delta is 1. This illustrate that the linear interdependence of the cover image and generated distribution is additional if the delta is 1.

II. *Performance Analysis of proposed VC scheme (Encryption Performance)*

This segment is used to examine the presentation of the anticipated customized Signcryption algorithm. The investigation is prepared by means of contrasting the generated distribution before encryption and after it is decrypted. Table 4 gives the contrast values of created shares.

Table 4: Contrast of created shares

Contrast of created shares					
Delta	**0.6**	**0.7**	**0.8**	**0.9**	**1**
Share 1	0.30605	0.305083	0.303681	0.303591	0.305169
Share 2	0.301712	0.304996	0.303597	0.303897	0.306015
Share 3	0.305424	0.304207	0.305292	0.303715	0.300769
Share 4	0.305875	0.303899	0.303269	0.304780	0.303502
Share 5	0.302265	0.303141	0.305488	0.305350	0.305873

Table 5 gives the contrast values of created shares after it is retrieved from decryption using Unsigncryption.

Table 5 Contrast of decrypted shares

Contrast of decrypted shares					
Delta	**0.6**	**0.7**	**0.8**	**0.9**	**1**
Decrypt 1	0.302265	0.303141	0.305488	0.305350	0.305873
Decrypt 2	0.302265	0.303141	0.305488	0.305350	0.305873
Decrypt 3	0.302265	0.303141	0.305488	0.305350	0.305873
Decrypt 4	0.302265	0.303141	0.305488	0.305350	0.305873
Decrypt 5	0.302265	0.303141	0.305488	0.305350	0.305873

In Tables 4 and 5, it is obviously observed that the dissimilarity of the innovative and decrypted distribution is remarkably different. But there is insignificant is similarity in the choice of 0.001 to 0.005. This illustrate the effectiveness of the anticipated format and performance. A smaller amount dissimilarity in expressions of the image dissimilarity among the recovered (decrypted) and innovative distributions.

III. *Performance Analysis of proposed VC based Extraction of secret data:*

In this segment, the presentation of the anticipated VC related removal of secret data is examined. Therefore, the NC value is calculated among the innovative and removed secret image. The calculated NC value is specified in the beneath Table 6.

Table 6: Normalized Correlation between original and extracted secret image

Normalized Correlation					
Delta	**0.6**	**0.7**	**0.8**	**0.9**	**1**
Twitter-logo (Retrieved Secret image)	0.997375	0.997131	0.997253	0.997314	0.997314

In Table 6, it is obvious that the NC is elevated if the delta is identical to 0.6. Additionally, the NC is 0.997314 for the delta values 0.9 and 1.0. On the other hand, the entire values are illustrating that the effectiveness of the anticipated algorithm is 0.997.

6. Conclusion

In this document, an effectual protected VC format is executed by the aid of customized Signcryption algorithm. The anticipated VC format is established to conquer the complexity to handle the insignificant distributions. Furthermore, the anticipated VC format offers elevated defense through signcrypting the consequential distributions and afterwards permitting decryption of distributions only if the password related validation is accomplished. The presentation of the anticipated VC format is investigated at each phase (i.e. for the period of embedding, after decryption, and for the period of removal) through examining the enhanced images. The consequence illustrates the exceptional presentation effectiveness of the anticipated process.

Compliance with Ethical Standards

Funding: This work is not funded by any agencies and the study is as part of the Ph.D degree

Conflict of Interest: The authors, Jinu Mohan and Dr Rajesh R declare that we have no conflict of interest

Ethical approval: This article does not contain any studies with human participants or animals performed by any of the authors.

References

[1] Ching-Nung Yang and Ting-Hao Chung, "A general multi-secret visual cryptography scheme", Optics Communications, vol. 283, no. 24, pp. 4949-4962, 2010.
[2] Xiaotian Wu and Wei Sun, "Generalized Random Grid and Its Applications in Visual Cryptography", IEEE Transactions on Information Forensics and Security, vol. 8, no. 9, pp. 1541-1553, 2013.
[3]]Ran-Zan Wang, Yung-ChingLan, Yeuan-KuenLee, Shih-Yu Huang, Shyong-JianShyu, and Tsorng-LinChia, "Incrementing visual cryptography using random grids", Optics Communications, vol. 283, no. 21, pp. 4242-4249, 2010.
[4] Xuehu Yan, Shen Wang and Xiamu Niu, "Threshold construction from specific cases in visual cryptography without the pixel expansion", Signal Processing,vol.105,pp.389-398,2014.
[5] V. Petrauskiene, R. Palivonaite, A. Aleksa and M. Ragulskis, "Dynamic visual cryptography based on chaotic oscillations", Communications in Nonlinear Science and Numerical Simulation, vol. 19, no. 1, pp. 112-120, 2014.
[6] Sian-Jheng Lin, Shang-Kuan Chen and Ja-Chen Lin, "Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion", Journal of Visual Communication and Image Representation, vol. 21, no. 8, pp. 900-916, 2010.
[7] Kai-Hui Lee and Pei-Ling Chiu, "A high contrast and capacity efficient visual cryptography scheme for the encryption of multiple secret images", Optics Communications, vol. 284, no. 12, pp. 2730-2741, 2011.
[8] Feng Liu, Teng guo, ChuanKun Wu and Lina Qian, "Improving the visual quality of size invariant visual cryptography scheme", Journal of Visual Communication and Image Representation, vol. 23, no. 2, pp. 331-342, 2012.
[9] Pei-Ling Chiu and Kai-Hui Lee, "User-friendly threshold visual cryptography with complementary cover images", Signal Processing, vol. 108, pp. 476-488, 2015.
[10] Ching-Nung Yang, Chih-Cheng Wu and Dao-Shun Wang, "A discussion on the relationship between probabilistic visual cryptography and random grid", Information Sciences, vol. 278, pp. 141-173, 2014.
[11] Dao-Shun Wang, Member, IEEE, Tao Song, Lin Dong, and Ching-Nung Yang, "Optimal Contrast Grayscale Visual Cryptography Schemes With Reversing", IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 2059-2072, 2013.
[12] Xuehu Yan, Shen Wang, Xiamu Niu and Ching-Nung Yang, "Generalized random grids-based threshold visual cryptography with meaningful shares", Signal Processing, vol. 109, pp. 317-333, 2015.
[13] Xiaotian Wu and Wei Sun, "Improved tagged visual cryptography by random grids", Signal Processing,vol. 97, pp. 64-82, 2014.
[14] Ming-Shi Wang and Wei-Che Chen, "A hybrid DWT-SVD copyright protection scheme based on k-means clustering and visual cryptography", Computer Standards & Interfaces, vol. 31, no. 4, pp. 757-762, 2009.
[15] Paulius Palevicius and Minvydas Ragulskis, "Image communication scheme based on dynamic visual cryptography and computer generated holography", Optics Communications, vol. 335,pp. 161-167, 2015