A New Bi-Level Encoding and Decoding Scheme for Pixel Expansion Based Visual Cryptography

Ram Chandra Barik, National Institute of Technology, Durgapur, India

Suvamoy Changder, National Institute of Technology, Durgapur, India

Sitanshu Sekhar Sahu, Birla Institute of Technology, Mesra, India

ABSTRACT

Mapping of image-based object textures to ASCII characters can be a new modification towards visual cryptography. Naor and Shamir proposed a new dimension of Information security as visual cryptography which is a secret sharing scheme among *N* number of participants with pixel expansion. Later on, many researchers extended the visual secret sharing scheme with no expansion of pixel regions in binary and color images. By stacking *k* shares the secret can be decoded using normal vision. In this paper the authors have proposed a modification towards visual cryptography by converting the message in the form of printable ASCII character-based numerical encoding patterns in a binary host image. The encoding of the message is represented as ASCII numeric and a texture of those numeric are arranged to form a binary host image. Then, *N* numbers of shares are built up but after stacking all the shares the decoding of the message is achieved by converting ASCII numeric to the secret.

KEYWORDS

ASCII Code, Binary Host Image, Lagrange's Interpolation, Visual Cryptography

INTRODUCTION

Demand of information exchange in heavy data traffic is increasing day by day with the influence of digital media over internet. Information security in modern era is a major concern for many mathematicians, computer scientists. For abstracting the secret from malicious access, third party attack there are many algorithms and mathematics was being proposed in last three decade. Usage of Mathematics makes many cryptographic algorithms robust. Today's world is roaming behind the information operated in electronic media and internet technology starting from banking sector (both offline and online banking) to multimedia industry. As advancement of electronic media, digital communication makes the world is in finger press at the same time misuse of information is a big threat to modern world. Cryptography makes the secret information into an unreadable format and plays a vital role in presence of third parties or eavesdropper for secure communication. In the last three decades, popular cryptographic algorithms RSA, AES, DES, Blowfish, Secret Sharing etc. using private key and public key concepts provides security to text-based information. Day by day evolution of digital multimedia information system demands to build new cryptographic algorithm to

DOI: 10.4018/IJRSDA.2019010102

cope with current technological arena. Steganography, Visual Cryptography, QR Code are emerging areas of security over modern multimedia technology. Visual Cryptography combines secret sharing scheme proposed by (Shamir 1979) with visual transparencies into n number of shares. The concept of visual cryptography is combined with visual secret sharing, threshold secret sharing scheme to produce a robust encryption and decryption method which has the broad areas of application. To divide secret data into shares which generate random shares of (k-1) polynomial degree using modulus based arithmetic where ($k \leq n$). f(x) can be derived in equation (1) as

$$f\left(x\right) = \left(a_0 + a_1 x^1 + a_2 x^2 \ldots + a_{k-1} x^{k-1}\right) \bmod p_r \tag{1}$$

Secret data is a_0, p_r is the prime number $p_r > a_0$ and $p_r > n$. From the integer values of uniformly distributed [1; p) the coefficients $\mathrm{a}_1, \mathrm{a}_2 \ldots \mathrm{a}_{k-1}$ are chosen randomly. Mathematically Lagrange's interpolation is used in secret sharing scheme which is represented in equation (2), (3) and (4) using Lagrange's interpolation $\left(x_i, f\left(x_i\right)\right)$, I = 1, 2…n.

$$f\left[x_0, x_1 \ldots, x_n, x\right] = 0 \tag{2}$$

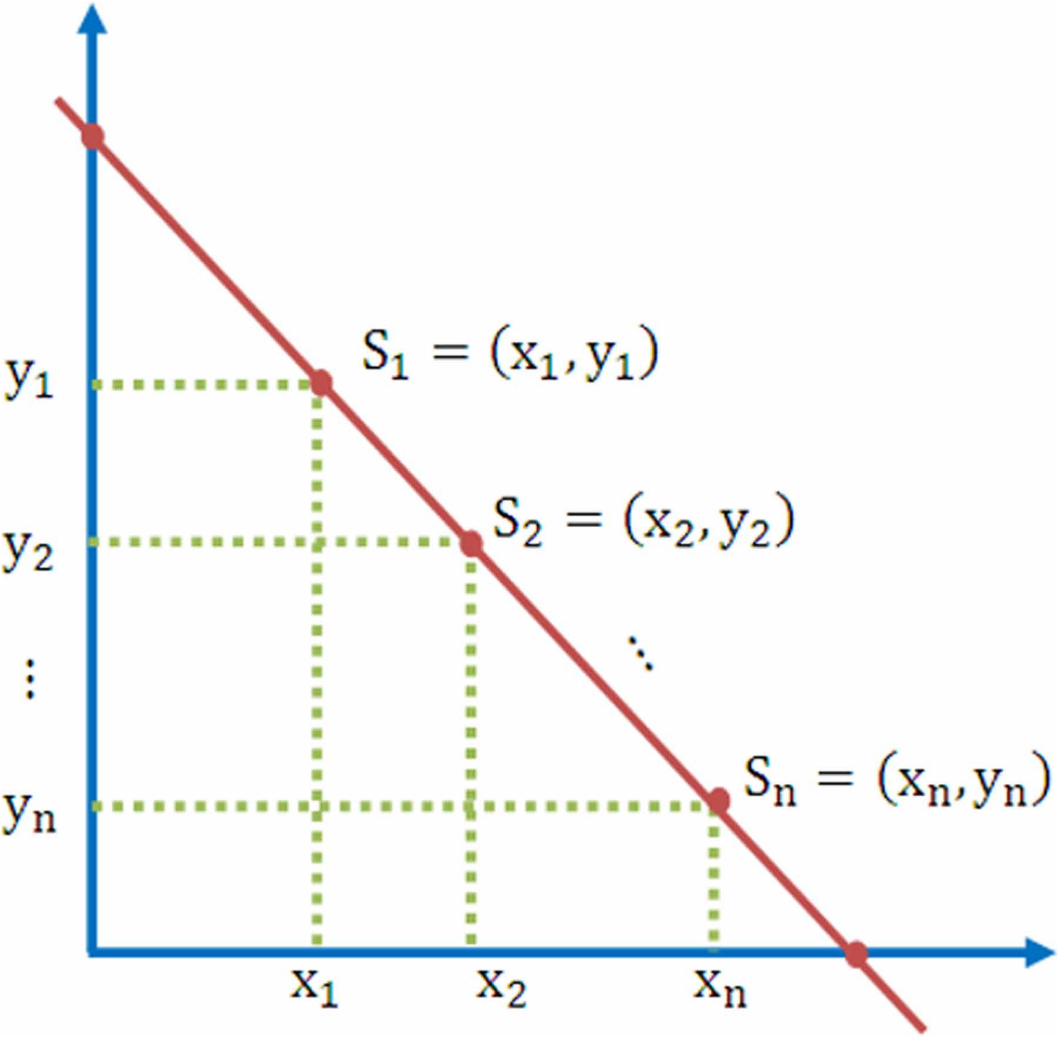
$$\mathrm{f}\left(\mathrm{x}\right) = \frac{\left(\mathrm{x} - \mathrm{x}_1\right)\ldots\left(\mathrm{x} - \mathrm{x}_n\right)}{\left(\mathrm{x}_0 - \mathrm{x}_1\right)\ldots\left(\mathrm{x}_0 - \mathrm{x}_n\right)} \mathrm{f}_0 + \ldots + \frac{\left(\mathrm{x} - \mathrm{x}_0\right)\ldots\left(\mathrm{x} - \mathrm{x}_{n-1}\right)}{\left(\mathrm{x}_n - \mathrm{x}_0\right)\ldots\left(\mathrm{x}_n - \mathrm{x}_{n-1}\right)} \mathrm{f}_n = \sum_{i=0}^{n} \left(\prod_{j=0}^{n} \frac{\mathrm{x} - \mathrm{x}_j}{\mathrm{x}_i - \mathrm{x}_j} \right) \mathrm{f}_i \tag{3}$$

$$\mathrm{y} = \mathrm{f}\left(\mathrm{x}\right) = \mathrm{secret}\left(\mathrm{s}\right) + \sum_{j=1}^{k-1} \mathrm{a}_j \mathrm{x}^j \tag{4}$$

Visual Cryptography gives a new dimension to information security arena using secret sharing scheme among a set of trusted participants. Beauty of this security concept is that unlike other highly computational with bigger complexity method such as RSA, AES, DES the decoding of the corresponding secret can be achieve using normal human perception without performing the computation at receivers end. Visual Cryptography has versatile application areas starting from banking sector to other security area.

Secret sharing scheme introduced by Naor and Shamir (Naor & Shamir 1995) is being modified in many dimensions with pixel expansion and no expansion. Binary image with the secret embedding inside black and white pixels intensity or grey level is encoded to form shares using binary patterns randomly. The shares are mapped onto transparencies and distributed between n participants as $\mathrm{P} = \left(\mathrm{P}_1,\ \mathrm{P}_2 \ldots\ \mathrm{P}_n\right)$. The distribution can be done in such a way to all qualified participants that the original message or secret is visible if k transparencies overlapped or stacked together. The message or secret is invisible when k-1 transparencies stacked even if a highly computational algorithm used. The Qualified participants which holds the share $\Gamma = \left\{\mathrm{Q}_1, \mathrm{Q}_2 \ldots \mathrm{Q}_m\right\}$ where each Qualified subsets is called as the access structure. (Ateniese, Blundo, DeSantis, Stinson 1999) The extension for Naor and Shamir method towards general Access structures give a new dimension to visual secret sharing scheme. For example, $\mathrm{P} = \left\{\mathrm{S1},\ \mathrm{S2},\ \mathrm{S3}\right\}$ with general access structure are qualified sets at least having two sub-sets as $\left\{\mathrm{S1}, \mathrm{S2}\right\}, \left\{\mathrm{S2}, \mathrm{S3}\right\}$. Whereas overall qualified participants are

Figure 1. Shows the (2, n) secret sharing scheme



$$\Gamma = \left\{\left\{S1, S2\right\}, \left\{S2, S3\right\}, \left\{S1, S2, S3\right\}\right\}$$

The rest of the subsets are restricted. For $\left(n,\ n\right)$ threshold scheme a dealer will distribute the secret SC_0 into n different participants. Let us assume SC_0 into belongs to a group G_s which holds the series of binary strings as message of length m with addition by module 2, i.e., $G_s\ =\ G_sF\left(2\right)^m$. By generating random sequence $SC_1,\ SC_2 \ldots\ SC_n$ in such a way that $\sum_{j=1}^{n} SC_j \rightarrow SC_0$. The shares are distributed among each j^{th} participants. Let us assume P be a set of participants. Power set of P as 2^P holds the access structure Γ_P which is a subset of this power set and it represent the genuine shares to decode the secrets. Every element of Γ_{P} and their superset also present in Γ_{P}. If X and Y are within P in such a way that $\mathrm{X} \subseteq \mathrm{Y} \subseteq \mathrm{P}$ and $\mathrm{X} \in \Gamma_{\mathrm{P}}$, $\mathrm{Y} \in \Gamma_{\mathrm{P}}$.

The contribution of the paper is organized as First any text message or secret is mapped into an ASCII numeric. This numeric is represented as it is a black background with white object texture arranged in a matrix form. This matrix is plotted as a 2-D covert host image embedding information as an ASCII numeric form. This image is now passed to (2, 2) visual cryptography phase to generate pixel scrambled and expanded shares or transparencies for encryption and distributed to n number of participants. For decryption or decoding all these shares are collected and stacked to recover or reconstruct the covert host image which is skewed towards left and right with very much sharp contrast embedding ASCII numeric. ASCII numeric is visually decoded to corresponding ASCII text by using ASCII chart.

BACKGROUND

The reconstructed image and its contrast for k out of m Visual cryptography scheme is measured by difference evaluation within the scheme. For each transparency m subpixels are used for the corresponding pixel expansion. A pair of $\mathrm{n} \times \mathrm{m}$ Boolean matrices generated as the basis matrices of k out of n threshold Visual Cryptography Scheme with pixel expansion m.

If $\Gamma_{\mathrm{Qual}} \subseteq 2^{\mathrm{P}}$ as represents qualified sets, $\Gamma_{\mathrm{Forb}} \subseteq 2^{\mathrm{P}}$ as forbidden sets. $\mathrm{P} = \left\{1, 2, \ldots \mathrm{n}\right\}$ are a set of participants with 2^{P} is power set which contain the subsets. Γ_{Qual} is increasing monotonically as the same time Γ_{Forb} is decreasing monotonically. $\Gamma_{Qual} \cup \Gamma_{Forb} = 2^{P}$, $\Gamma_{Qual} \cap \Gamma_{Forb} = \varnothing$. A participant $\mathrm{p} \in \mathrm{P}$ is crucial participant $\exists\ \mathrm{X} \subseteq \mathrm{P}$ such that $\mathrm{X} \cup \left\{\mathrm{p}\right\} \in \Gamma_{\mathrm{Qual}}$ but $\mathrm{X} \notin \Gamma_{\mathrm{Qual}}$. If a participant is not crucial then share will not be allotted to him or her (Ateniese, Blundo, DeSantis & Stinson 1999; Zhou, Arce & Crescenzo, 2006).

Definition1: For a set of n participants assume $\left(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}}\right)$ be the access structure there exists two collection of Boolean matrix of size $\mathrm{n} \times \mathrm{m}$ as C_0 &C_1 which constitutes a Visual Cryptography scheme if there exists a value $\pm\left(\mathrm{m}\right)$ and t_{X} for every X and satisfies the below two circumstance of protocol as

Protocol for Contrast level: Any (qualified) set $\mathrm{X} = \left\{\mathrm{i}_1, \mathrm{i}_2, \ldots, \mathrm{i}_{\mathrm{a}}\right\} \in \Gamma_{\mathrm{Qual}}$ with a participants stacked the shared transparencies to recover the secret shared image. Formally we can define $\mathrm{M} \in \mathrm{C}_{0,1}$ the row vectors $\mathrm{V}_{0,1}\left(\mathrm{X}, \mathrm{M}\right)$ as the OR of the rows $\mathrm{r}_{\mathrm{i1}}, \mathrm{r}_{\mathrm{i2}}, \mathrm{r}_{\mathrm{i3}} \ldots \mathrm{r}_{\mathrm{ia}}$ in M. Which can be expressed as $\acute{\mathrm{E}}\left(\mathrm{V}_0\left(\mathrm{X}, \mathrm{M}\right)\right) \leq \mathrm{t}_{\mathrm{X}} - \pm\left(\mathrm{m}\right).\mathrm{m}\ \forall\ \mathrm{M} \in \mathrm{C}_0$ and $\acute{\mathrm{E}}\left(\mathrm{V}_1\left(\mathrm{X}, \mathrm{M}\right)\right) \geq \mathrm{t}_{\mathrm{X}}\ \forall\ \mathrm{M} \in \mathrm{C}_1$.

Protocol for Security level: Any (forbidden) subset $\mathrm{X} = \left\{\mathrm{i}_1, \mathrm{i}_2, \ldots, \mathrm{i}_{\mathrm{b}}\right\} \in \Gamma_{\mathrm{Forb}}$ with b participants having no information of the secret image. Formally, the two collections of $\mathrm{b} \times \mathrm{m}$ matrices $\mathrm{D}_{0,1}$ formed by extracting rows $\left\{\mathrm{i}_1, \mathrm{i}_2, \ldots, \mathrm{i}_{\mathrm{b}}\right\}$ from each matrix in C_0 and C_1. t_{X} is the threshold to visually recognize the reconstructed pixel as black or white which can be derived as $\mathrm{t}_{\mathrm{X}} = \min\left(\acute{\mathrm{E}}\left(\mathrm{V}_1\left(\mathrm{X}, \mathrm{M}\right)\right)\right)$ overall matrices $\mathrm{M} \in \mathrm{C}_1$.

The relative difference $\pm\left(\mathrm{m}\right)$ can be derived as

$$\pm\left(\mathrm{m}\right) = \frac{\min\left(\acute{\mathrm{E}}\left(\mathrm{V}_1\left(\mathrm{X}, \mathrm{M}\right)\right)\right) - \max\left(\acute{\mathrm{E}}\left(\mathrm{V}_0\left(\mathrm{X}, \mathrm{M}\right)\right)\right)}{\mathrm{m}} \text{over all X and M} \tag{5}$$

Based on the secret pixel s as white or black the matrix M is randomly selected from C_0 and C_1 respectively.

Definition 2: By permuting the columns of two basis matrix S^0 and S^1 in all possible ways the two collection matrix C_0 and C_1 is obtained. Both the basis matrix S^0 and S^1 satisfies the below protocol as

Protocol for Contrast level: if $X = \{i_1, i_2, \ldots, i_a\} \in \Gamma_{Qual}$ then the row vector V_0 and V_1 obtained by performing OR operation on rows $r_{i1}, r_{i2}, r_{i3} \ldots r_{ia}$ of S^0 and S^1 respectively by satisfying equation 6

$$\acute{E}\left(V_0\left(X, M\right)\right) \leq t_X - \pm\left(m\right).m \text{ and } \acute{E}\left(V_1\left(X, M\right)\right) \geq t_X \tag{6}$$

Protocol for Security level: if $X = \{i_1, i_2, \ldots, i_b\} \in \Gamma_{Forb}$ one of the two $b \times m$ matrices by extracting rows $\{i_1, i_2, \ldots, i_b\}$ from S^0 and S^1 with the column permutation.

Dealer randomly chooses subpixels in one row of a matrix in the set C_0 which includes all matrices permuted by the columns in B_0 (Similarly for C_0 includes all matrices permuted by columns in B_1). OR vector of any r rows in B_i can be obtained using OR $\left(B_i \mid r\right)$, i= 0, 1. H (.) is the Hamming weight function then (k, n) Visual Cryptography Scheme should satisfy both security and contrast condition.

Example 1(Yang et. al 2010): Generate a (2, 2) Visual Cryptography Scheme of h=1, l=0 & m=2 using $B_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$ & $B_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

$$H\left(OR\left(B_1|2\right) = 2\right),\ H\left(OR\left(B_0|2\right) = 1\right), H\left(OR\left(B_1|1\right)\right) = H\left(OR\left(B_0|1\right)\right) = 1$$

Satisfies both security (forbidden) and contrast condition. As black color can be distinguished from white as “m−h”B“h”W and white color as “m−l”B“l”W, the xByW is represented for $\begin{pmatrix} x & y \\ 1\cdots1 ' & 0\cdots0 \end{pmatrix}$ and its permutations. The reconstructed image with a white color is 1B1W and black color is 2B0W. Every 2-subpixel block in shadows (noise like) is 1B1W.

For a (2, 2) VCS with 2 participants and their shares are required to map or reconstruct secret with recovered image size may vary to 2 or 4 times larger than the covert image. Due to effect of distorted aspect ratio every pixel splited to four sub pixels as 2×2 array. Where every share is looks in the visual form in Figure 1. White pixel is formed using two identical arrays from Figure 2 and Black pixel is formed using two complementary arrays from Figure 3. By stacking both shares together the result is white (Medium Grey) or Black (Complementary Black).

The pixel expansion scheme has its pros and cons over visual cryptography. The procedure of expanding of pixel during share generation is now modified by many researchers with no pixel expansion. Table1 shows the Expansion of Pixel during share generation and its “OR” Operation over both white and Black pixel. Pixel overlapping will occur after pixel stacking or super positioning the random shares or transparencies.

(Yang & Chen, 2008) Color Mixing in a probabilistic way with extended CVCSs with price reducing on contrast quality to certain level. Whiteness or brightness is a tuning parameter to discriminate the color used in Probabilistic Visual Cryptography Scheme in black and white areas.

Figure 2. The horizontal, vertical, and diagonal shares

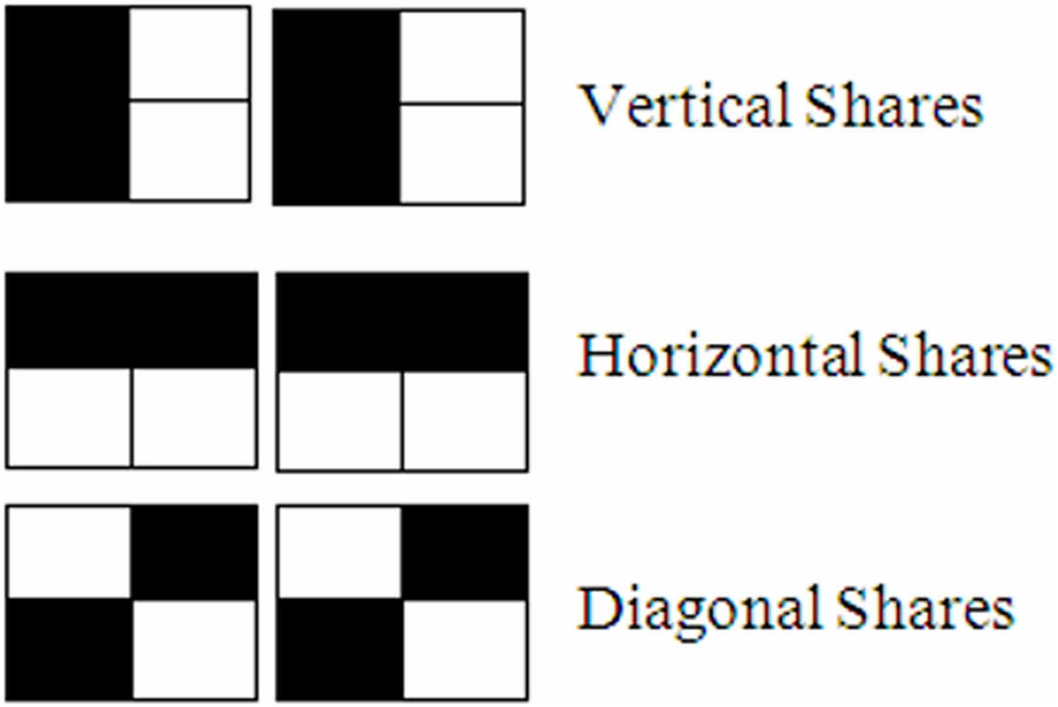


Figure 3. The horizontal, vertical, and diagonal shares

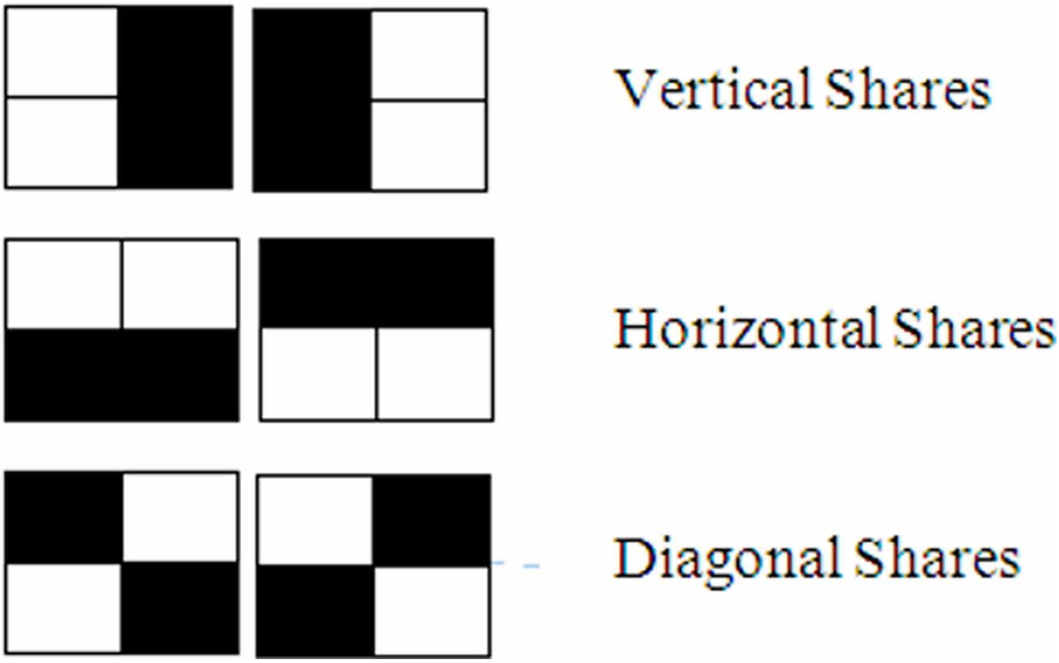


Table 1. Expansion of Pixel during share generation and its OR Operation

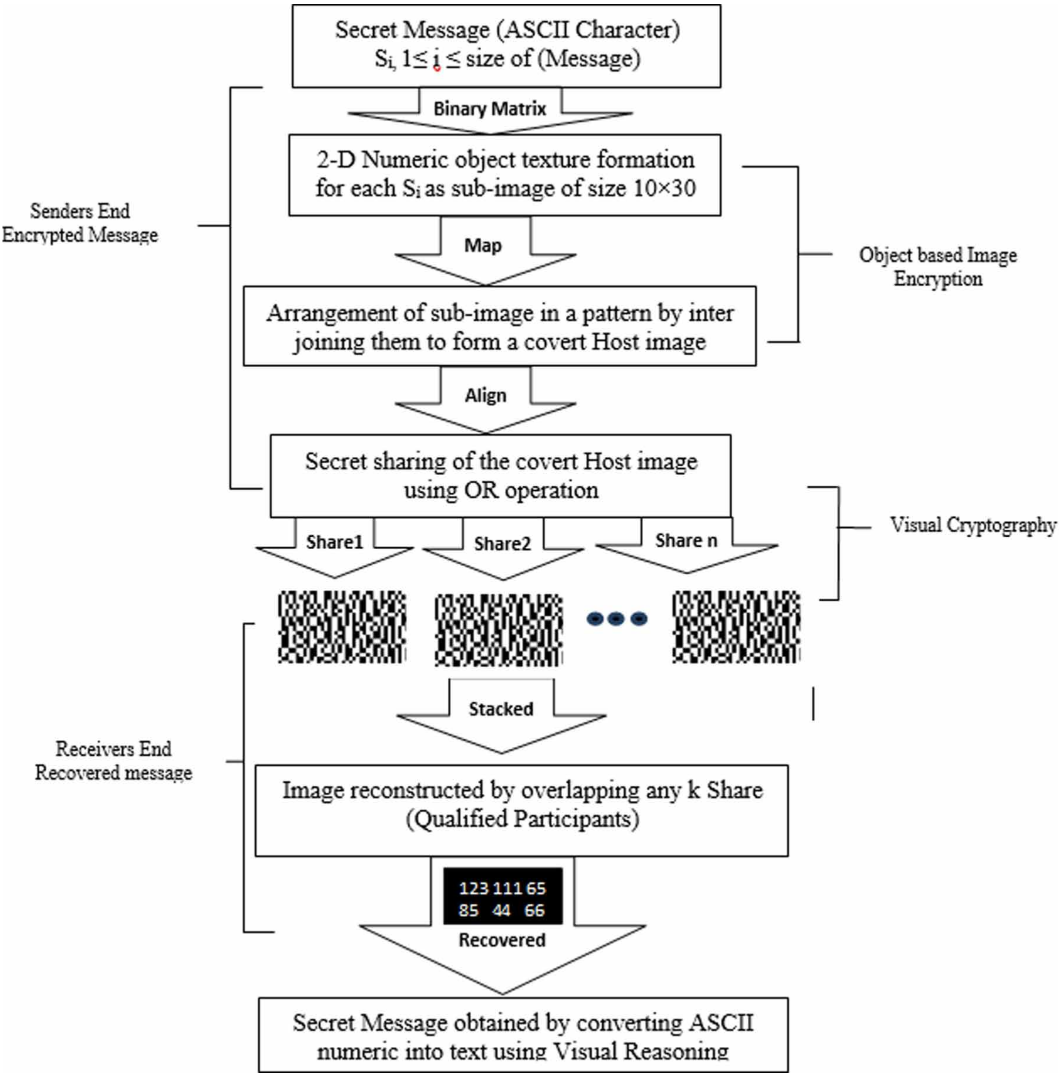
Pixel Grey level	Probability	Share 1	Share 2	Superimpose
□	50%	□■	□■	□■
	50%	■□	■□	■□
■	50%	□■	■□	■■
	50%	■□	□■	■■

(Liu, Wu & Lin, 2010) contrast of the Visual Cryptography Scheme (VCS) is shown to be inappropriate. Liu et al. proposed a new definition of the contrast based on observations. (Yang & Chung, 2010) When secret image is more than one then Multi secret Visual Cryptography Scheme (MVCS) which can be applied on any k and n, and it gives the formal security and contrast conditions of (k, n)-MVCS and satisfies the security and contrast conditions. (Liu & Wu, 2011) meaningful shares or images embedded as random shares and the secret can be visually recovered by stacking qualified subset $\left(\Gamma_{\text{Qual}}\right)$. Liu proposed threshold covering subset optimality black ratio and the procedure to improvise the visual quality of the share images. (Liu, Wu & Lin, 2011) cheating immune visual cryptography schemes (CIVCS) are an extension of Traditional VCS to avoid the cheating while secret image is recovered. Lee and Chiu (2012) Extended Visual Cryptography Scheme for general access structures. EVCS add meaningful transparencies or cover in each share it. (Lee et al., 2014) proposed an algorithm to encode halftone secret image using non pixel expansion Visual secret sharing scheme which can be applied into versatile images such as normal image, brighter and darker image. (Tsai, Chen & Horng, 2007) A cheating prevention scheme using multiple secret images. The 2-out-of-n threshold scheme is used to show the feasibility of the proposed scheme. The secret images are recovered from the respective qualified subsets and the other secret images will be unknown to potential cheaters. (Ito, Kuwakado & Tanaka, 1999) A new visual cryptography algorithm proposed with Image size invariant property (no pixel expansion). (Chen, Chan, Huang, Tsai & Chu, 2007) A multiple-level visual secret-sharing scheme(MLVSS) binary halftone share images is obtained by encoding a grey-level secret image into. Every share will have equal-sized block which is created by MLVSS scheme. Contrast Quality is marginable using MLVSS scheme using after reconstruction of the image. (Chen, Horng & Tsai, 2012), Chen. et. al. proposed cryptanalyzed a cheating-prevention scheme in VC and have shown that it is not cheating immune. Forge transparencies are barred to cheat. Base matrix need to be find out.

PROPOSED METHOD

Architectural flow depicts the skeletal view of the proposed work. This paper introduces a new modification to existing Visual Cryptography technique. In the proposed method the encoding process comprises two phases or steps. The message is mapped to the sub images with binary smooth texture of ASCII numeric for example the message "*a b*" is represented as "*097 032 098*" in the first phase. Between the string "*a space b*" the single character "*a* = 97", "*space* = 32", "*b* = 98". In the second phase then by using Visual Cryptography method *n* number of shares or transparencies is created for *k* participant. But decoding of the secret will be obtained after successfully the random shares need to be super positioned properly. Figure 4 shoes the architectural flow of the o

Figure 4. The architectural flow of the proposed algorithm


Secret Message (ASCII Character)
S_i, 1≤ i ≤ size of (Message)
Binary Matrix
2-D Numeric object texture formation for each S_i as sub-image of size 10×30
Map
Arrangement of sub-image in a pattern by inter joining them to form a covert Host image
Align
Secret sharing of the covert Host image using OR operation
Share1
Share2
Share n
Senders End Encrypted Message
Object based Image Encryption
Visual Cryptography
Stacked
Receivers End Recovered message
Image reconstructed by overlapping any k Share (Qualified Participants)
123 111 65
85 44 66
Recovered
Secret Message obtained by converting ASCII numeric into text using Visual Reasoning

Algorithm

Algorithms are the finite step by step procedure to resolve to a computational problem in theoretically. In this paper the algorithm is decomposed into two parts one is encoding and another is decoding scheme.

Encoding Scheme

```
(a)         Input and output phase
Input: Message to be encode, Message size, Mapped ASCII numeric
Output: Shuffled Shares with pixel scrambling.
(b)         Encryption phase
Step 1: Convert Array of Secret Message into the corresponding
ASCII numeric value for each character.
Step 2: Map the ASCII numeric into binary smooth texture and plot
```

```
it as sub-image of size 10×30 using below procedure
Sub Procedure Image_object_texture (Digit=4, n)
// Digit represents between ‘0’ and ‘9’ to be form texture of Sub-
image
Declare a matrix as Four [10][10];
Four → zero (10, 10); // Black background of sub-image and will be
ones (10, 10) for reverse
Four (2:9, 9) → 1; // 0 for reverse
Four (6, 4:9) → 1; // 0 for reverse
i → 6;
j → 4;
while ((i>=2) and (j<=9)) // Iteration Start
Four (i, j) → 1; // Four (i, j) → 0 for white background and black
foreground color
i → i-1;
j → j+1;
end // Iteration end
end // End of Procedure
Step 3: Arrange the sub-images into a 2-D binary image based on
message size if Message is (1×16 → 4×4) or (1×32 → 8×4). This is
the First level encoding.
Step 4: Generate n numbers of shares from the Original image
using Visual cryptography. The shares are noisy like images or
transparencies with pixel expansion.
Step 5: The shares are distributed to n number of participants.
```

Decoding Scheme

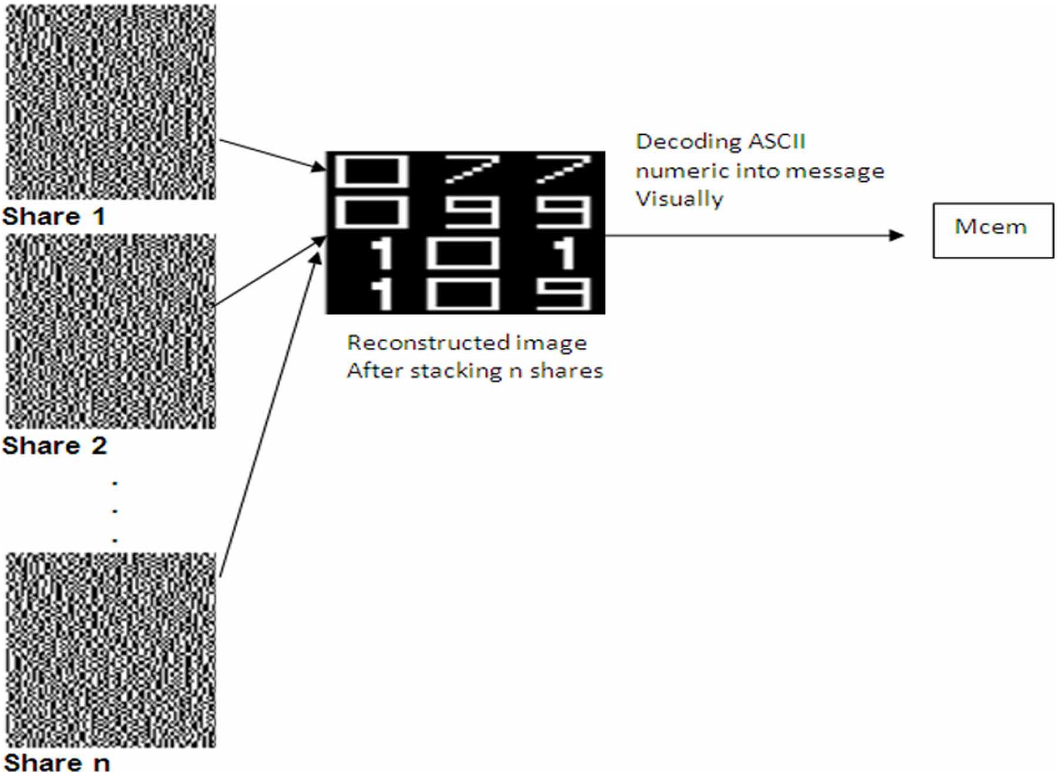
```
(a)         Input and output phase
Input: k pixel scrambled shares.
Output: Resultant Image.
(b)         Decryption phase
Step 1: Collect all the shares from n participants.
Step 2: Stack all n number of shares so that one reconstructed and
recovered image with pixel expansion will be obtained.
Step 3: The recovered image with the ASCII numeric object texture
embedded inside it.
Step 4: Visually map the ASCII numeric texture into corresponding
ASCII character following ASCII chart hence the secret information
will be obtained.
```

Decryption of cipher text into plain text is a prominent aspect of any cryptographic algorithm. In the proposed algorithm the decryption is bi-level procedure. As per the protocol the decryption in visual cryptography is processed visually. In level 1 the n number of shares are stacked to reconstruct the image which conceal ASCII numeric based binary object texture which is visible to the user. In level 2 the deciphering object representing ASCII numeric digit is mapped to plain text or original message. Figure 5 demonstrates the overall process.

Image Texture Formation for Printable Character - ASCII Based

The proposed binary image-based encryption method which embeds information or message as visual texture in the form of ASCII character. The image holds the concealed message. The smooth visual texture in a sub image made of binary pixels represents for each ASCII character is the mapping of

Figure 5. Depicts overall decryption process



the original message. The visual textures are formed starting from printable character Space with ASCII value as 32 to tilde with ASCII value 126 which is depicted in Table 2.

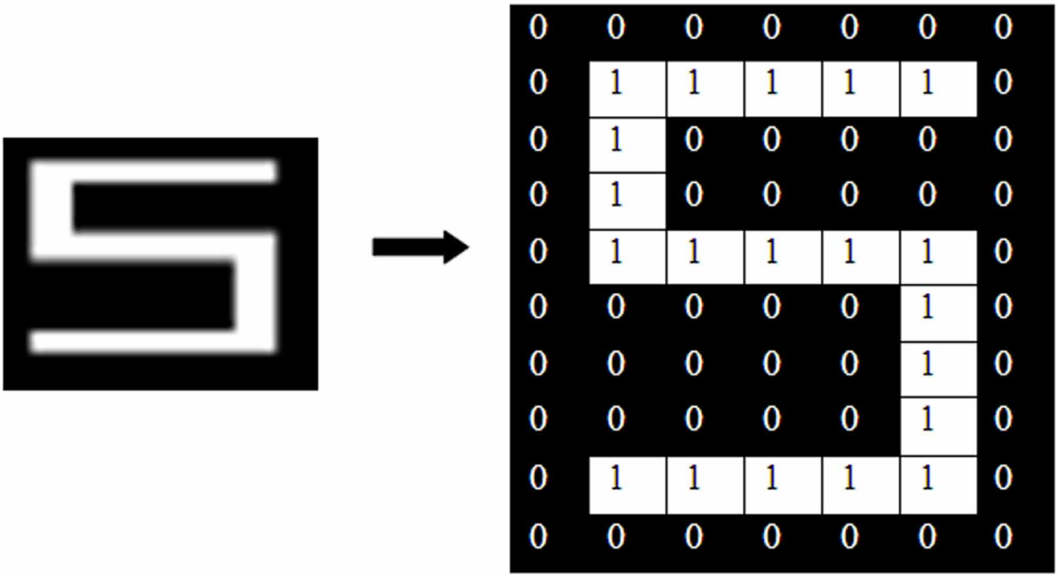
Primarily a matrix of a matrix of N×N pixels with values zero (0) as intensity representing black background is created which can be realized as an image Im(x, y) having black foreground as well as black background. Over the black background the foreground objects are represented as white symbolic object. Mathematically image Im(x, y) can be shown in equation 7 that describes the formation of binary image. For example Figure 6 represents the binary texture of digit 5 in an image form.

$$\mathrm{Im}(x, y) = \mathrm{Mat}_{ij} \begin{cases} = 1 \, for\, points\, on\, the\, object \\ = 0 \, for\, background\, points \end{cases} \tag{7}$$

Intensity zero (0) represent as black and intensity one (1) represent as white in a binary image. The visual objects texture are represented in as sub binary images that is stored in both sender and receiver side. The image in the form of binary matrix (N×N pixels) splits into small blocks of the sub images or matrix having size 10×30 (n=10 × m=30). The original matrix size is based on the message which needs to organize into an image form. Many intelligence methods do recognize the digits from the image using digit recognition. This is achieved by converting the curved texture of digits into straight line-based texture to predict correctly.

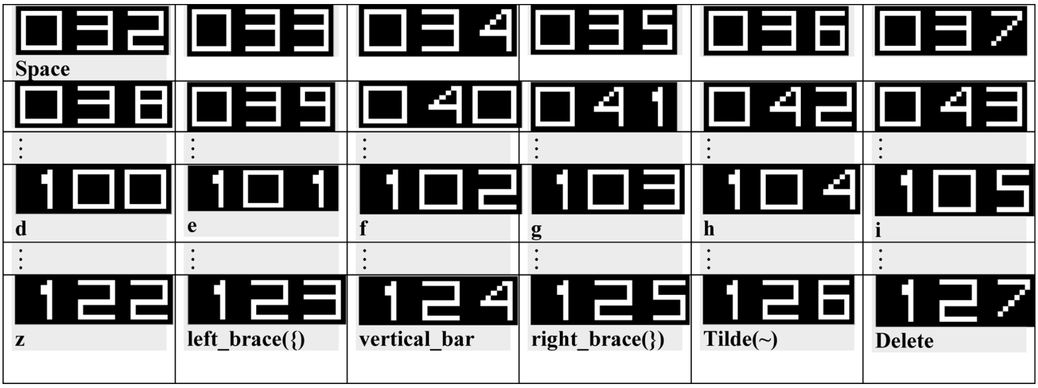
The sub images are inter-joined in row and column format to form a host image embedding the ASCII printable character as visual texture. Mathematically the inter-joining is represented in Equation 8.

Figure 6. The binary image representation and formation of digit 5



0	0	0	0	0	0	0
0	1	1	1	1	1	0
0	1	0	0	0	0	0
0	1	0	0	0	0	0
0	1	1	1	1	1	0
0	0	0	0	0	1	0
0	0	0	0	0	1	0
0	0	0	0	0	1	0
0	1	1	1	1	1	0
0	0	0	0	0	0	0

Table 2. Contains the Texture for ASCII character Space (32) to (tilde) 127



032 Space	033	034	035	036	037
038	039	040	041	042	043
⋮	⋮	⋮	⋮	⋮	⋮
100 d	101 e	102 f	103 g	104 h	105 i
⋮	⋮	⋮	⋮	⋮	⋮
122 z	123 left_brace({)	124 vertical_bar	125 right_brace(})	126 Tilde(~)	127 Delete

$$\sum_{i=1}^{n} \mathrm{subIm}\left[\mathrm{i}\right]_{10\times 30} \rightarrow \text{Covert Host Image} \tag{8}$$

Where $\mathrm{subIm}\left[\mathrm{i}\right]_{10\times 30}$ represents the sub-images $\forall\ \mathrm{i} = 1, 2, \ldots \mathrm{n}$ which inter-join to form host image. Original message comprises the text as printable ASCII Character etc.

Figure 7. shows how a message of 1×16 is converted and reorganized into 4×4 array of ASCII numeric

$$\begin{bmatrix}\text{Min cipher image}\end{bmatrix}_{1\times16} \Rightarrow \begin{bmatrix} M & i & n & \\ c & i & p & h \\ e & r & & i \\ m & a & g & e \end{bmatrix}_{4\times4} \Rightarrow \begin{bmatrix} 77 & 105 & 110 & 32 \\ 99 & 105 & 112 & 104 \\ 101 & 114 & 32 & 105 \\ 109 & 97 & 103 & 101 \end{bmatrix}_{4\times4}$$

SIMULATION RESULTS AND DISCUSSION

The proposed encoding and decoding method extends the visual cryptography concepts to a new dimension. The proposed method encodes the data without any complex key like highly computational cryptographic algorithm. The flow of the proposed method is depicted in Figure 4.

The proposed method of encoding and decoding works with below steps.

Image Texture creation of numeric Objects

First each character of the secret message is mapped to corresponding ASCII numeric. Then texture for the each numeric between 0 and 9 is formed over a black and white background for example if the ASCII character for space is 32 can have texture as 032 using line and rectangle. Instead of embedding the character texture the corresponding ASCII numeric is embedded.

Formation of Covert Host Image

According to the algorithm the secret message is first converted into corresponding ASCII numeric and then for each numeric the image texture embedded in a matrix of 10×30 which is to be reorganized to form a Covert cipher Host image in such a way that the message of size 16 character will be denoted as 4×4. For example the message is "*Min cipher image*" then it can be arranged as shown in Figure 7 where as Figure 8 depicts the actual representation in a cipher host image by the arrangement of ASCII numeric values against the message.

Visual Share Creation

Visual cryptography is a new dimension of over traditional cryptography of private and public key encryption such as RSA, DES, and AES. The empirical analysis is to generate k shares (In this paper basically k=2). The information or secret image will be recovered by superimposing k shares as transparencies but < k shares will not reveal any secret. For visual share creation here the OR operation over the permutation of matrix column used. The shares look like a noisy transparencies or image by pixel scrambling.

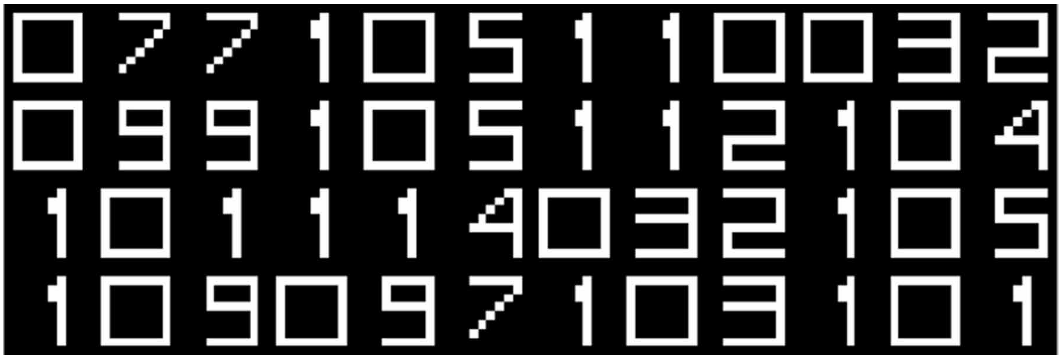
Case Study 1

In this case study for empirical analysis the authors first taken 16 characters based secret message which is to be reorganized into a matrix of 4×4. Then for each character is mapped to the ASCII numeric.

Encryption Phase

For simulation initially 16 characters based message "Mail-info@x1.com" is taken. ASCII numeric is mapped from each character of the message. After arranging the character into a block of 4×4 the ASCII numeric code is represented as graphical object embedded in an image of 10×30 size. For example space has the ASCII numeric code as 32 which can be represented as 032. As a whole

Figure 8. Conversion of Message as ASCII numeric sub image assemble to form host covert image in black background and white foreground objects



for 4×4 array each row has the size as 10×120 and after reorganized in the form of black and white image as Figure 9 clearly shows the binary host image embedding the information or secret into a series ASCII numeral. The binary image has the size 40×120 pixels representing 16 character secret messages. Up to this step one level encoding has been done but other level encoding is processed in the form of visual secret sharing denoted as visual cryptography. Two random shares are being generated using pixel permutation of columns with pixel expansion method in such a way that each share has the scaled size with respect to the width represented in Figure 10 and 11. Mathematically it can be denoted as matrix form in equation 9.

$$\begin{bmatrix} M_{10\times30} & M_{10\times30} & \cdots & M_{10\times30} \\ M_{10\times30} & M_{10\times30} & \cdots & M_{10\times30} \\ \vdots & \vdots & \vdots & \vdots \\ M_{10\times30} & M_{10\times30} & M_{10\times30} & M_{10\times30} \end{bmatrix}_{40\times120} \rightarrow \begin{bmatrix} M_{10\times60} & M_{10\times60} & \cdots & M_{10\times60} \\ M_{10\times60} & M_{10\times60} & \cdots & M_{10\times60} \\ \vdots & \vdots & \vdots & \vdots \\ M_{10\times60} & M_{10\times60} & M_{10\times60} & M_{10\times60} \end{bmatrix}_{40\times240} \quad (9)$$

Decryption Phase

The decryption is a bi fold process where k shares or transparencies with pixel expansion are stacked or super positioned to reconstruct or recover the secret image. Here the secret image is the host image which embeds secret message or information of size 1×16 in the form of ASCII numeric which is clearly shown in Figure 12. As VCS employs visual secret data (pictures, text, etc) which are undergoes to encryption phase but the condition is that the decryption of data does not require any computation rather human visual system is sufficient to decode. But in this paper after the stacking of k shares the recovered image does not contain the message as text directly rather the ASCII numeric of the corresponding text is being embedded as visual texture of numeric data will be show which does not require any computation but by using an ASCII chart the numeric coding could be decoded. It uses human visual system with human reasoning to decrypt the secret. Table 3 describes the mapping of ASCII numeric value into its text as secret.

Case Study 2

In this case study for empirical analysis the author first taken 32 characters based secret message which is to be reorganized into a matrix of 8×4. Then for each character is mapped to the ASCII numeric.

Figure 9. Texture of Message mapped to form ASCII code shown as Black and White image

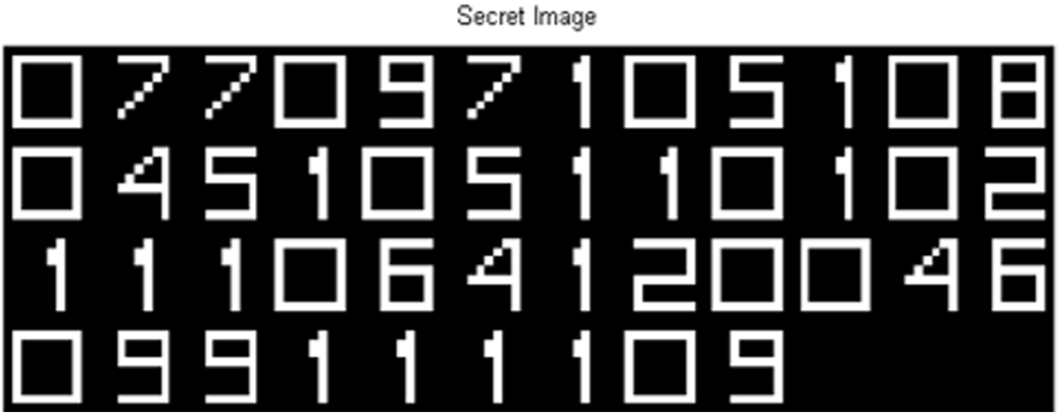


Figure 10. Share1 generation using VCS

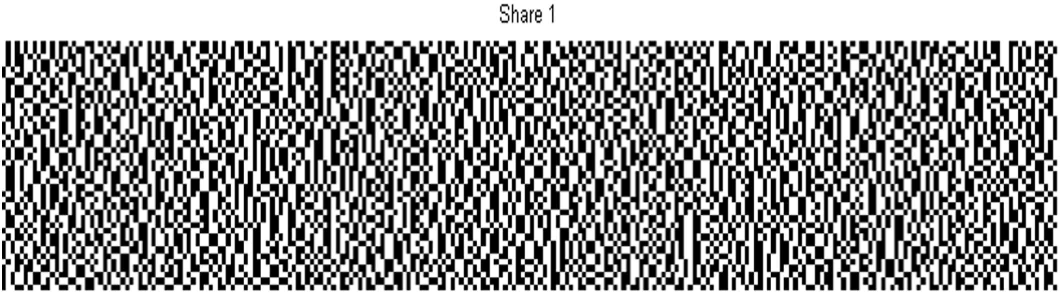


Figure 11. Share2 generation using VCS

Encryption Phase

In this case simulation initially 32 characters-based message “Mail-info@x1.com *Cryptography 123*” is taken. ASCII numeric is mapped from each character of the message. After arranging the character into a block of 4×4 the ASCII numeric code is represented as graphical object embedded in an image of 10×30 size. For example space has the ASCII numeric code as 32 which can be represented as 032. As a whole for 4×4 array each row has the size as 10×120 and after reorganized in the form of black and white image as Figures 13,14, and 15 clearly shows the binary host image embedding the information or secret into a series ASCII numeral. The binary image has the size 80×120 pixels

Figure 12. After stacking all shares, the recovered shown as Black and White image

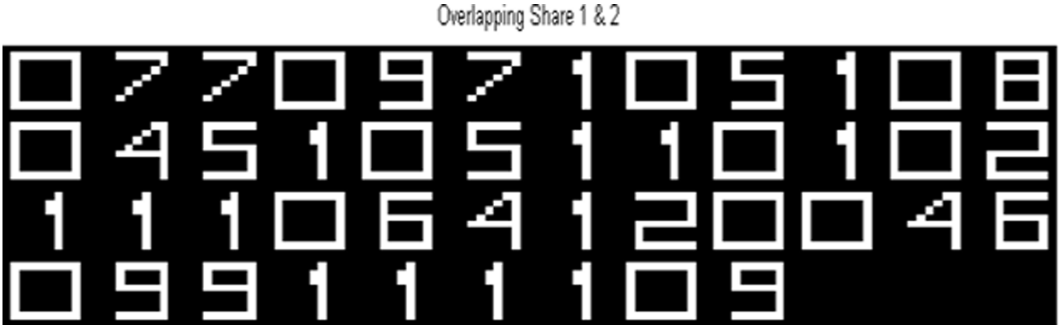


Table 3. The decoding pattern form ASCII numeric to corresponding ASCII character where message size is 16 characters

077 → M	097 → a	105 → i	108 → l
045 → –	105 → i	110 → n	102 → f
111 → o	064 → @	120 → x	046 → .
099 → c	111 → o	109 → m	

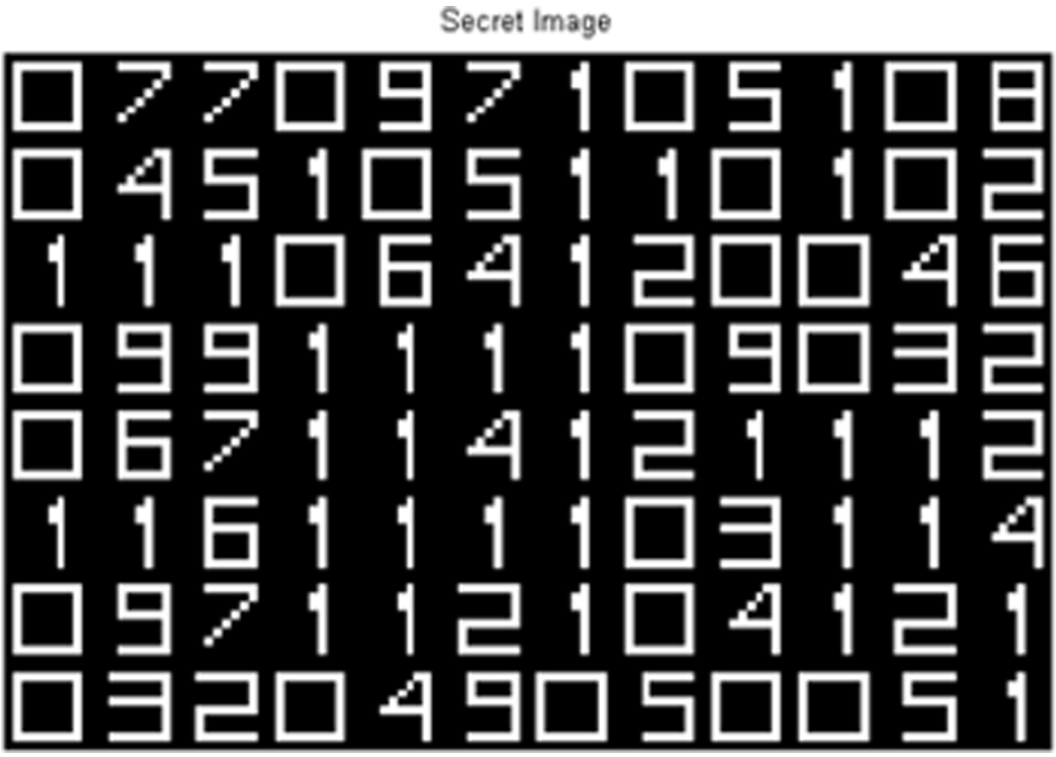
representing 16 character secret messages. Up to this step one level encoding has been done but other level encoding is processed in the form of visual secret sharing denoted as visual cryptography. Two random shares are being generated using pixel permutation of columns with pixel expansion method in such a way that each share has the scaled size with respect to the width. Mathematically it can be denoted as matrix form in equation 10.

$$\begin{bmatrix} M_{10\times30} & M_{10\times30} & M_{10\times30} \\ M_{10\times30} & M_{10\times30} & M_{10\times30} \\ \vdots & \vdots & \vdots \\ M_{10\times30} & M_{10\times30} & M_{10\times30} \\ M_{10\times30} & M_{10\times30} & M_{10\times30} \\ \vdots & \vdots & \vdots \\ M_{10\times30} & M_{10\times30} & M_{10\times30} \end{bmatrix}_{80\times120} = \begin{bmatrix} M_{10\times60} & M_{10\times60} & M_{10\times60} \\ M_{10\times60} & M_{10\times60} & M_{10\times60} \\ \vdots & \vdots & \vdots \\ M_{10\times60} & M_{10\times60} & M_{10\times60} \\ M_{10\times60} & M_{10\times60} & M_{10\times60} \\ \vdots & \vdots & \vdots \\ M_{10\times60} & M_{10\times60} & M_{10\times60} \end{bmatrix}_{80\times240} \tag{10}$$

Decryption Phase

Here the secret image is the host image which embeds secret message or information of size 1×32 in the form of ASCII numeric which is clearly shown in Figure 16 shows the encryption of information in the form of ASCII numeric. But in this paper after the stacking of k shares the recovered image does not contain the message as text directly rather the ASCII numeric of the corresponding text is being embedded as visual texture of numeric data will be show which does not require any computation but by using an ASCII chart the numeric coding could be decoded. It uses human visual system with human reasoning to decrypt the secret.

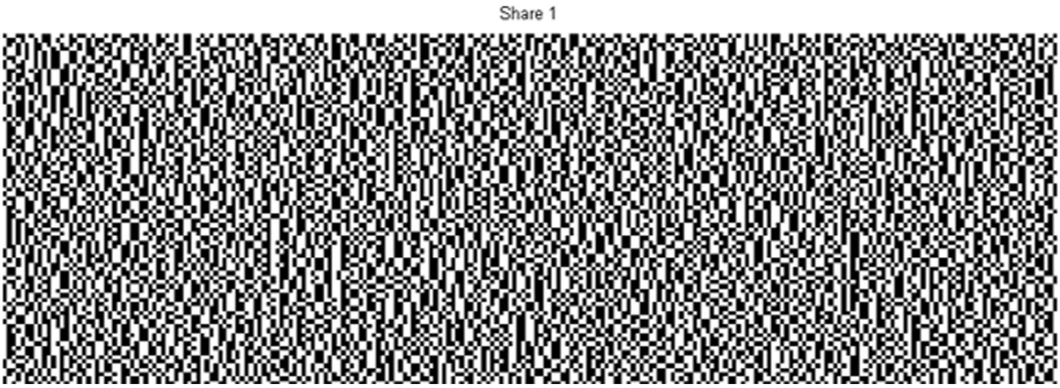
Figure 13. Texture of Message (1×32) mapped to form ASCII code shown as Black and White image



Secret Image

077097105108
045105110102
111064120046
099111109032
067114121112
116111103114
097112104121
032049050051

Figure 14. Share1 generation using VCS



Share 1

Generally, the decryption of Visual Cryptography is done visually without the use of computer but in this paper the authors has moved a step ahead to extend that visual based decoding to visual reasoning based decoding by merely using an ASCII chart. Mapping of each ASCII numeric texture of recovered image shown in Figure 16 into the 32-byte text is mapped in Table 4.

Message is “ Mail-info@x.com Cryptography 123 ”

Figure 15. Share2 generation using VCS

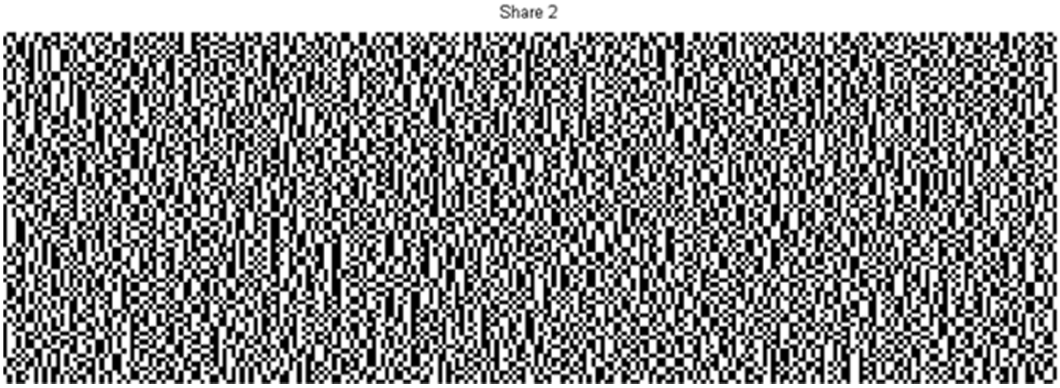


Figure 16. Shows the reconstructed image from the stacking of shares (Share1+Share2)

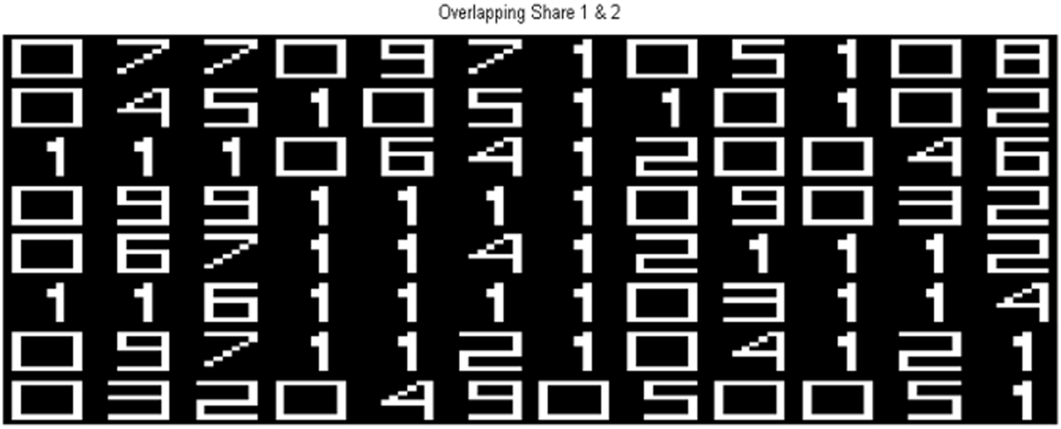


Table 4. The decoding pattern form ASCII numeric to corresponding ASCII character

077 → M	097 → a	105 → i	108 → l
045 → –	105 → i	110 → n	102 → f
111 → o	064 → @	120 → x	046 → .
099 → c	111 → o	109 → m	032 → Space
067 → C	114 → r	121 → y	112 → p
116 → t	111 → o	103 → g	114 → r
097 → a	112 → p	104 → h	121 → y
032 → Space	049 → 1	050 → 2	051 → 3

Case Study 3

In this case study for empirical analysis we have first taken 32 characters based secret message which is to be reorganized into a matrix of 8×4. Then for each character is mapped to the ASCII numeric. The image has white background and texture of ASCII numeric is black.

Encryption Phase

In this case simulation initially 32 characters-based message "Mail-info@x1.com *Cryptography 123*" is taken. ASCII numeric is mapped from each character of the message. After arranging the character into a block of 4×4 the ASCII numeric code is represented as graphical object embedded in an image of 10×30 size. For example, space has the ASCII numeric code as 32 which can be represented as 032. As a whole for 4×4 array each row has the size as 10×120 and after reorganized in the form of black and white image. Figure 17, 18, and 19 clearly shows the binary host image embedding the information or secret into a series ASCII numeral. The binary image has the size 80×120 pixels representing 16-character secret messages. Up to this step one level encoding has been done but other level encoding is processed in the form of visual secret sharing denoted as visual cryptography. Two random shares are being generated using pixel permutation of columns with pixel expansion method in such a way that each share has the scaled size with respect to the width. Mathematically it can be denoted as matrix form in equation 11.

$$\begin{bmatrix} M_{10\times30} & M_{10\times30} & M_{10\times30} \\ M_{10\times30} & M_{10\times30} & M_{10\times30} \\ \vdots & \vdots & \vdots \\ M_{10\times30} & M_{10\times30} & M_{10\times30} \\ M_{10\times30} & M_{10\times30} & M_{10\times30} \\ \vdots & \vdots & \vdots \\ M_{10\times30} & M_{10\times30} & M_{10\times30} \end{bmatrix}_{80\times120} = \begin{bmatrix} M_{10\times60} & M_{10\times60} & M_{10\times60} \\ M_{10\times60} & M_{10\times60} & M_{10\times60} \\ \vdots & \vdots & \vdots \\ M_{10\times60} & M_{10\times60} & M_{10\times60} \\ M_{10\times60} & M_{10\times60} & M_{10\times60} \\ \vdots & \vdots & \vdots \\ M_{10\times60} & M_{10\times60} & M_{10\times60} \end{bmatrix}_{80\times240} \tag{11}$$

Decryption Phase

Here the secret image is the host image which embeds secret message or information of size 1×32 in the form of ASCII numeric which is clearly shown in Figure 20 shows the encryption of information in the form of ASCII numeric. But after the stacking of k shares the recovered (reconstructed) image does not contain the message as text directly rather the ASCII numeric of the corresponding text is being embedded as visual texture of numeric data which is depicted in Figures 17, 18, and 19 does not require any computation but by using an ASCII chart the numeric coding could be decoded. It uses human visual system with human reasoning to decrypt the secret.

Message is "Mail-info@x.com Cryptography 123"

In case study1 input of message size with 16 characters (128 bits) used for ASCII based encryption but in case of case study2 input of message size with 32 characters (256 bits) used. As every ASCII character comprises binary texture of sub-image 10×30 pixel long.

Entropy & Histogram Analysis

Entropy is the measurement of statistics of randomness in terms of percentage of disorder which analyze the texture of the image. Table 6 shows the entropy variation of the proposed method with secret message of 16-character text and 32 character text. Histogram Analysis is effective when more number of grey levels is present in the image. By doing Histogram Equalization and Specification the

Figure 17. Texture of Message (1×32) mapped to form ASCII code shown as Black and White image

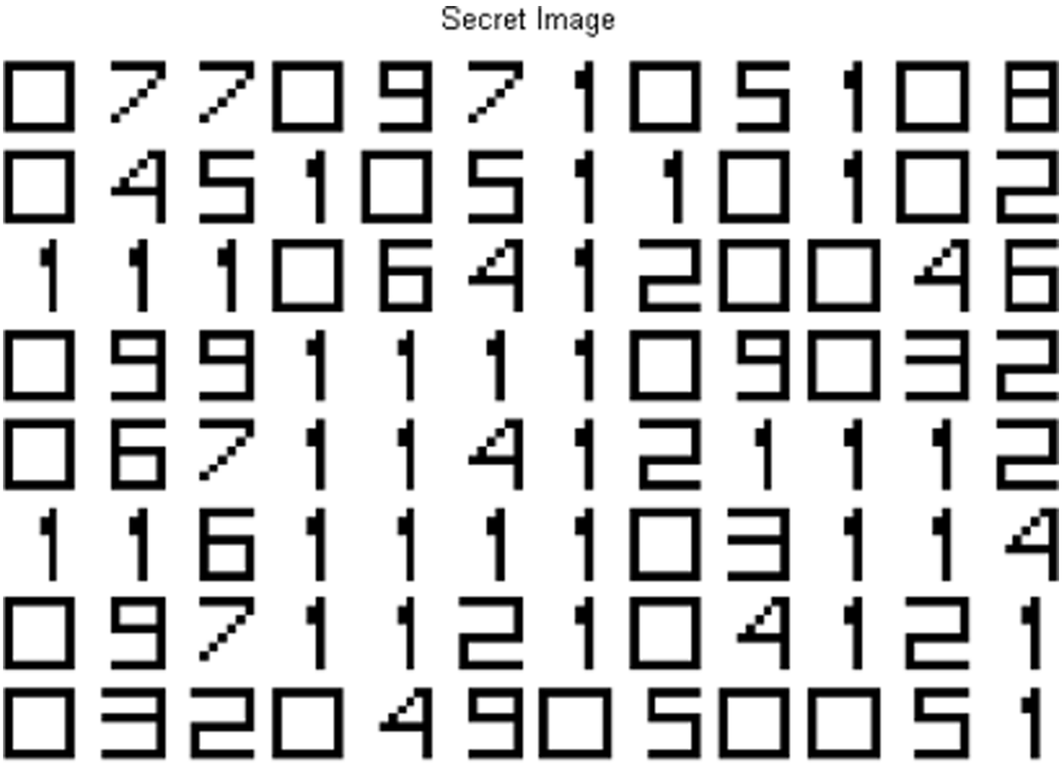
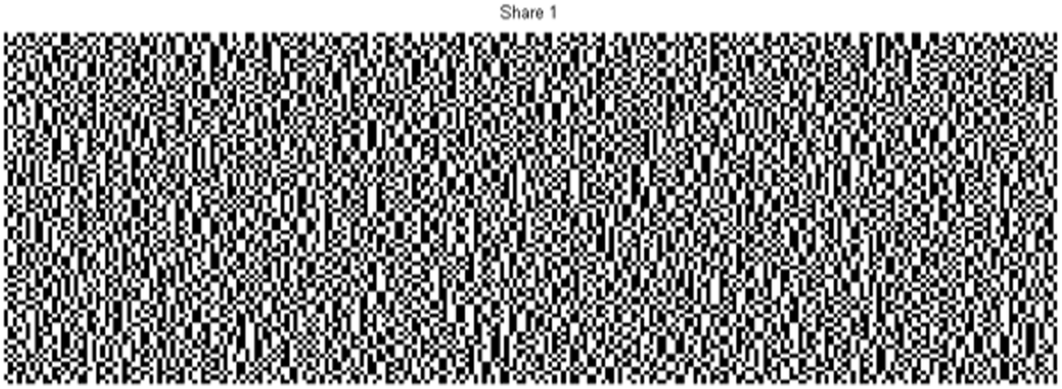


Figure 18. Share1 generation using VCS



Probability Density Function (PDF) is normalized to all grey levels. In this paper the covert image embeds the message into first level of encoding using ASCII code over a Black as background color and white as the foreground object texture color. So, the grey level here is logical means either on or off as Boolean values 1 or 0 which is displayed in Figure 21, 22, and 23. In case of a grey image the grey level is L-1(7 or 255).

Figure 19. Share2 generation using VCS

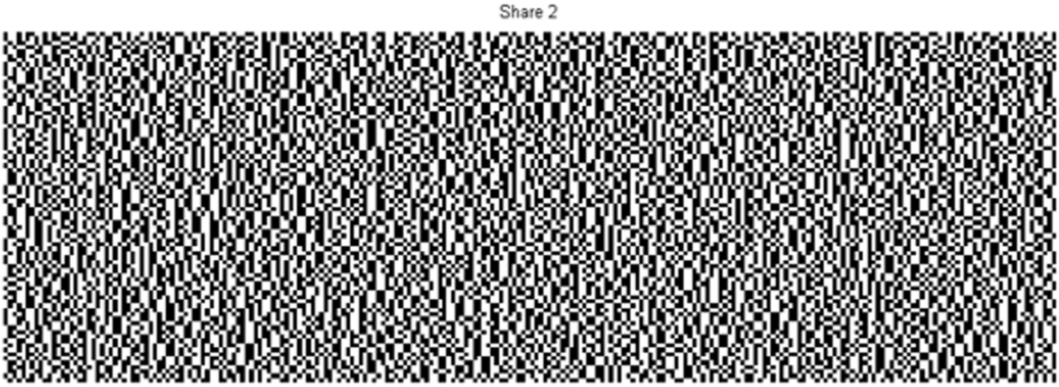


Figure 20. The reconstructed image from the stacking of shares (Share1+Share2)

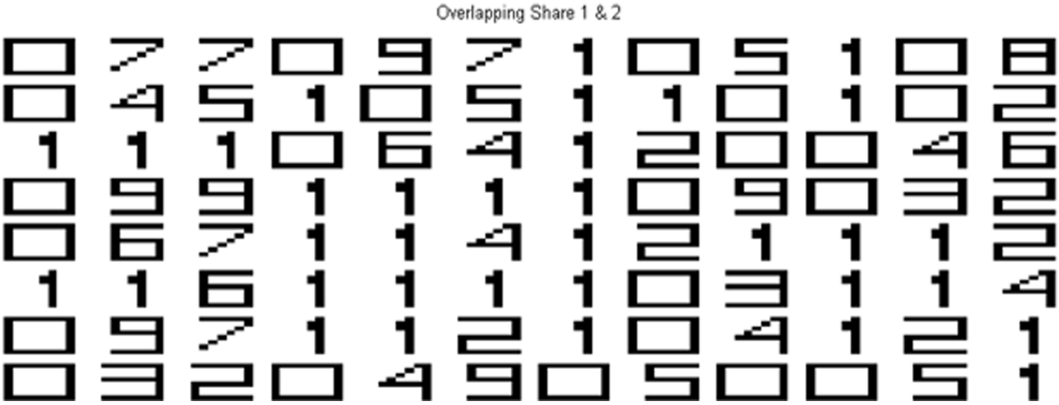


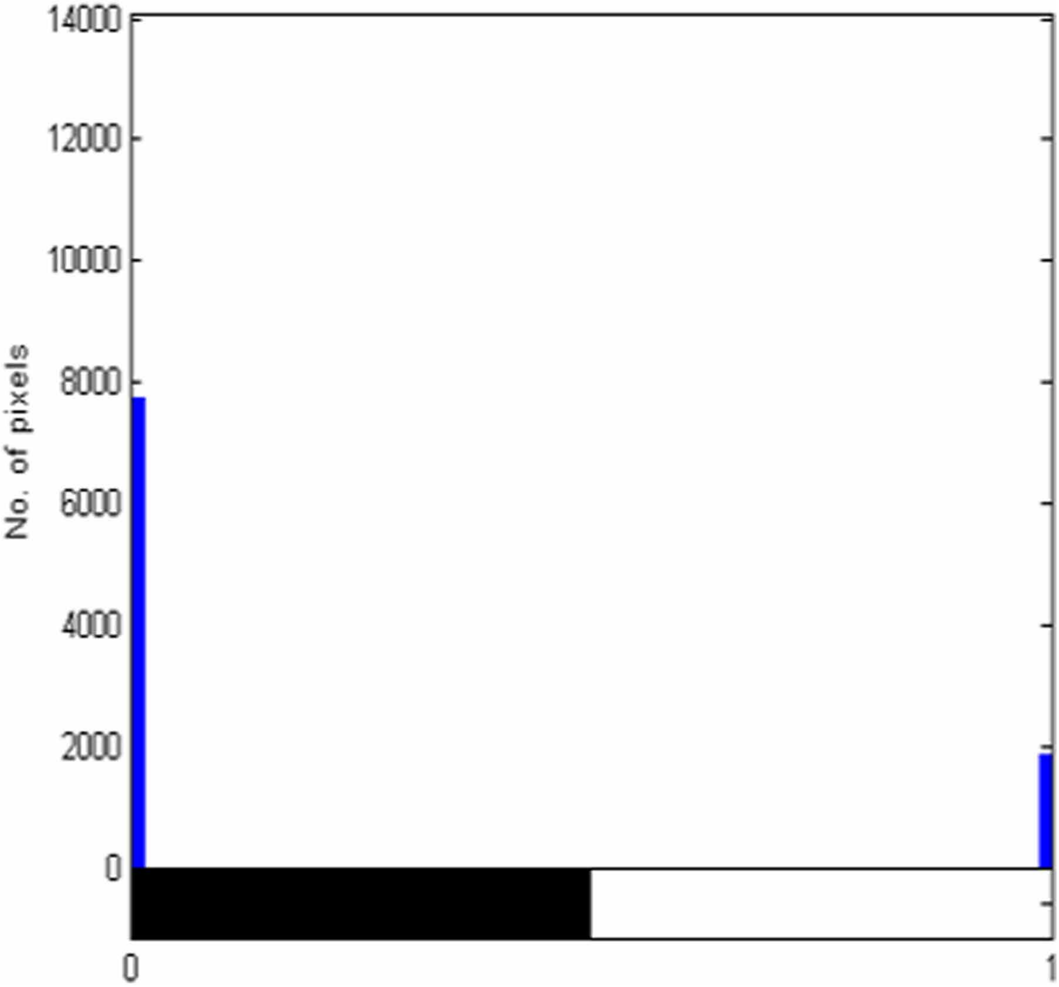
Table 5. Shows the decoding pattern form ASCII numeric to corresponding ASCII character

077 → M	097 → a	105 → i	108 → l
045 → –	105 → i	110 → n	102 → f
111 → o	064 → @	120 → x	046 → .
099 → c	111 → o	109 → m	032 → Space
067 → C	114 → r	121 → y	112 → p
116 → t	111 → o	103 → g	114 → r
097 → a	112 → p	104 → h	121 → y
032 → Space	049 → 1	050 → 2	051 → 3

Table 6. The entropy variation between original host image to reconstructed and recovered image

Message	Entropy		
	Original Host Image	Shares or Transparencies	Reconstructed & Recover Image
Message size(16)	0.6927	1	0.6927
Message size(32)	0.7062	1	0.7062

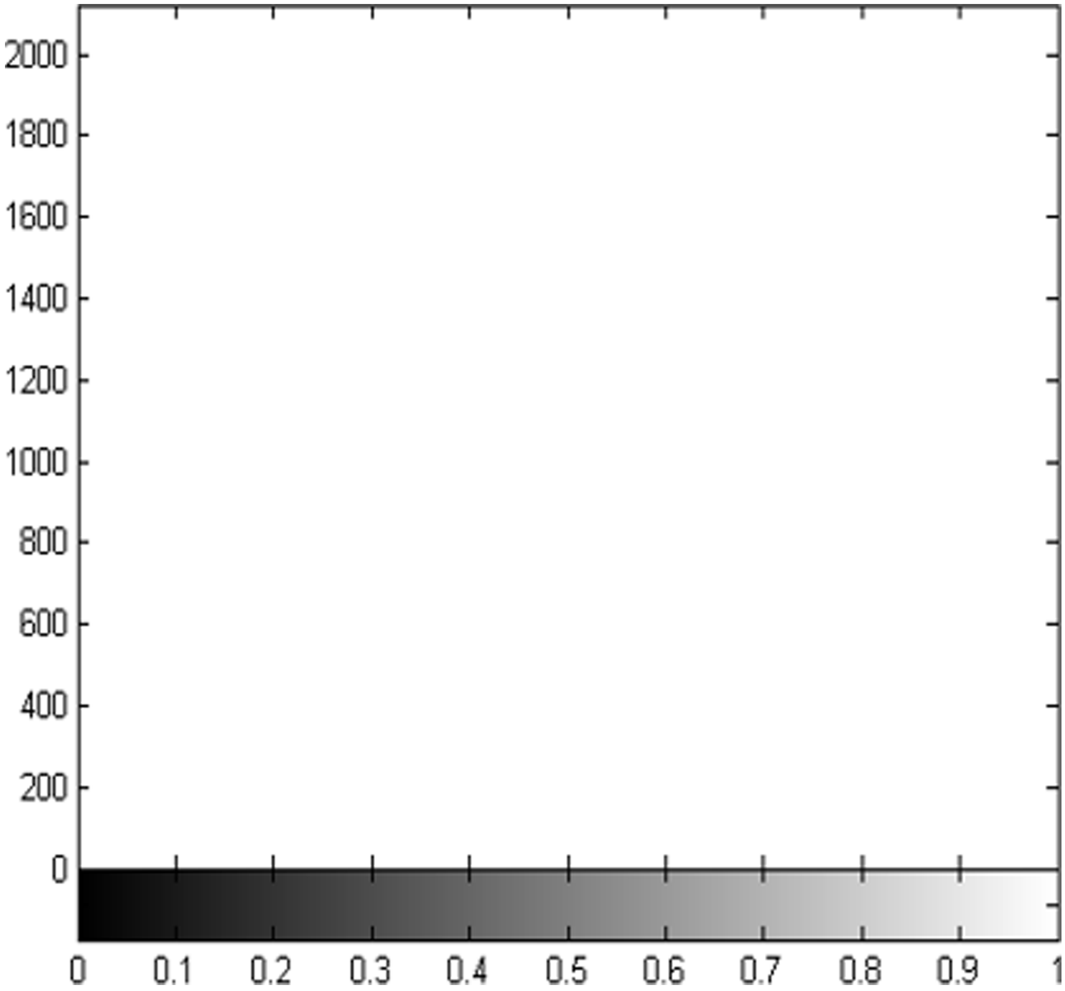
Figure 21. Original Host image



Histogram represent probability distribution of each grey level but as it is binary image the variation is between 0 to 1 only. Here histogram plotting is shown in Figures 21, 22, and 23. From the figure it is clear that both the plotting of original Host image and reconstructed image is almost similar.

Empirical analysis for any contribution towards research is essential. In this paper as a new diversion is being approached using ASCII numeric. The comparison with different methods is given in Table 7. Here the comparison is based on the message type to describe the nature of the message for encryption whether it is a secret image or text message embedded in an image. The major

Figure 22. Random shares



difference with other method is to decode the message from the reconstructed image which embeds the ASCII numeric mapping into corresponding ASCII text again it does not require computation rather a visual mapping.

CONCLUSION

In this paper a novel approach toward Visual cryptography is presented where two levels of encoding and two levels of decoding is processed. The decoding of the message is performed simultaneously using visual perception and ASCII chart but a major factor to be noticed that still the proposed method do not require computation for decode rather just a mapping of the numeric texture of ASCII code into corresponding text as the secret message. Fidelity criteria are a major quality concern for any image processing algorithm. The proposed method embeds the ASCII numeric as object texture in a black and white image which is made up of straight line but these line can be scaled to larger extent to satisfy fidelity criteria. With comparison to other method the proposed method is equivalent in all dimensions in terms of security and contrast parameter.

Figure 23. Recovered Image

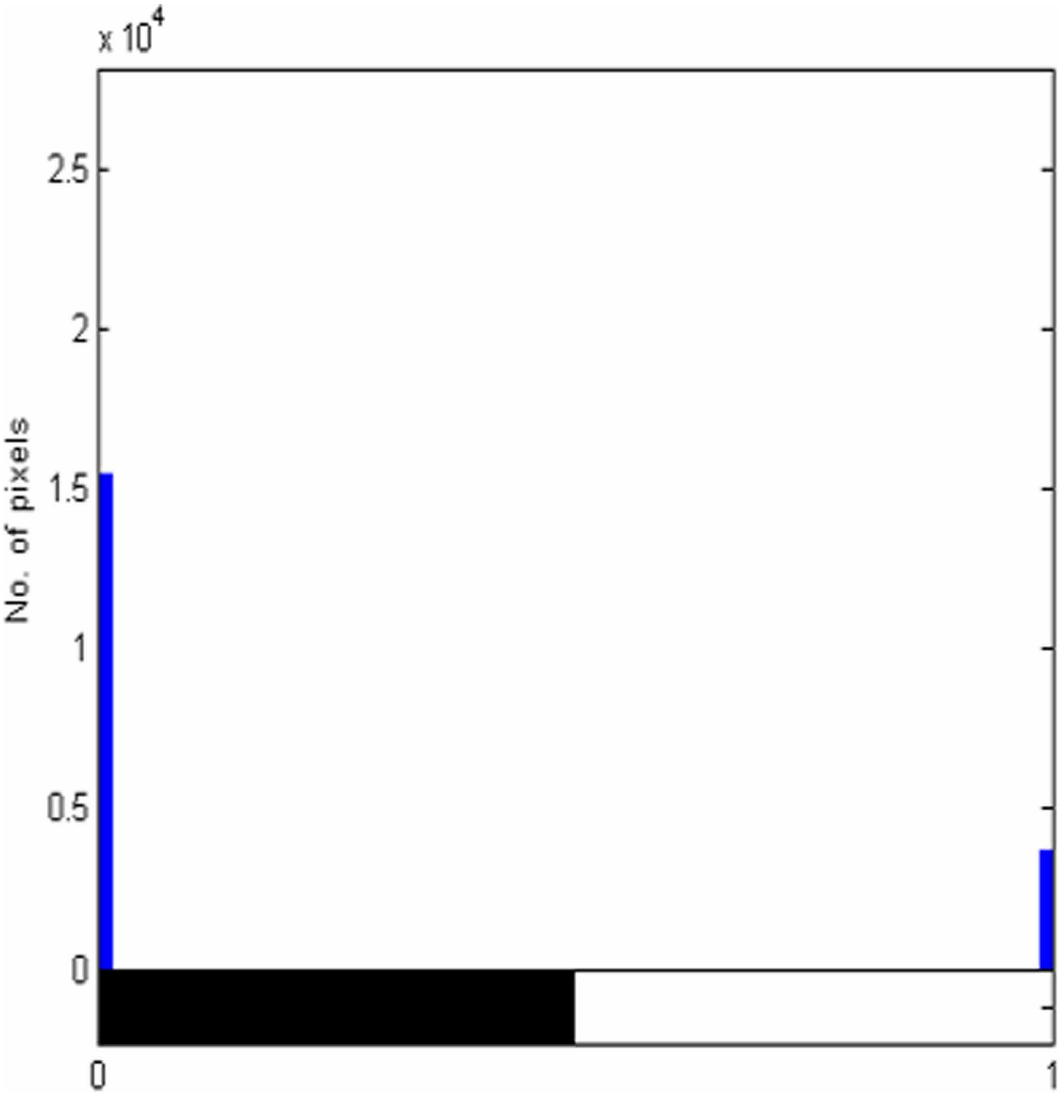


Table 7. Comparative analysis with existing VC scheme

Methods	Comparison Factors					
	Message Type	**Pixel Expansion**	**Nature of Shares**	**Visual effect of recovered image**	**Decoding Procedure**	**Security**
Ito et al. (1999) scheme	Covert image embedding message or image	NO	Noise –like/ Pixel Scrambled	Low	Visual Perception	Resistance to attacks
Chen et al. (2012) scheme	Covert image embedding message or image	YES	Noise –like/ Pixel Scrambled	High	Visual Perception	Resistance to attacks
Liu et al. (2011) scheme	Covert image embedding message or image	YES	Noise –like/ Pixel Scrambled	High	Visual Perception	Resistance to attacks
Proposed Scheme	Covert image embedding message using ASCII numeric	YES	Noise –like/ Pixel Scrambled	High	Visual Perception + ASCII Chart	Resistance to attacks

REFERENCE

Ateniese, G., Blundo, C., DeSantis, A., & Stinson, D. R. (1999). Visual Cryptography for General Access Structures. *Information and Computation*, *129*(2), 86–106. doi:10.1006/inco.1996.0076

Chen, Y. C., Horng, G., & Tsai, D. S. (2012). Comment on "Cheating Prevention in Visual Cryptography." *IEEE Transactions on Image Processing*, *21*(7), 3319–3323. doi:10.1109/TIP.2012.2190082 PMID:22410333

Chen, Y. F., Chan, Y. K., Huang, C. C., Tsai, M. H., & Chu, Y. P. (2007). A multiple-level visual secret-sharing scheme without image size expansion. *Inform. Sci.*, *177*(21), 4696–4710. doi:10.1016/j.ins.2007.05.011

Hu, C. M., & Tzeng, W. G. (2007). Cheating prevention in visual cryptography. *IEEE Transactions on Image Processing*, *16*(1), 36–45. doi:10.1109/TIP.2006.884916 PMID:17283763

Ito, R., Kuwakado, H., & Tanaka, H. (1999). Image size invariant visual crypto-graphy. *IEICE Transaction Fundamental Electronic Communication Computing*, *10*, 2172–2177.

Lee, C. C., Chen, H. H., Liu, H. T., Chen, G. W., & Tsai, C. S. (2014). A new visual cryptography with multi-level encoding. *Journal of Visual Languages and Computing*, *25*(3), 243–250.

Lee, K. H., & Chiu, P. L. (2012). An Extended Visual Cryptography Algorithm for General Access Structures. *IEEE Transactions on Information Forensics and Security*, *7*(1), 219–229.

Liu, F., & Wu, C. (2011). Embedded Extended Visual Cryptography Schemes. *IEEE Transactions on Information Forensics and Security*, *6*(2), 307–322.

Liu, F., Wu, Ch., & Lin, X. (2010). A new definition of the contrast of visual cryptography scheme. *Information Processing Letters*, *110*(7), 241–246. doi:10.1016/j.ipl.2010.01.003

Liu, F., Wu, C., & Lin, X. (2011). Cheating immune visual cryptography scheme. *IET Information Security*, *5*(1), 51–59. doi:10.1049/iet-ifs.2008.0064

Naor, M., & Shamir, A. (1995). Visual Cryptography. In *Advances in Cryptology—Eurocrypt '94 of Lecture Notes in Computer Science* (pp. 1–12). Berlin: Springer-Verlag. doi:10.1007/BFb0053419

Shamir, A. (1979). How to share a secret. *Communications of the ACM*, *22*(11), 612–613. doi:10.1145/359168.359176

Tsai, D. S., Chen, T. H., & Horng, G. B. (2007). A cheating prevention scheme for binary visual cryptography with homogeneous secret images. *Pattern Recognition*, *40*(8), 2356–2366. doi:10.1016/j.patcog.2007.01.013

Yang, C. N., & Chen, T. S. (2008). Colored visual cryptography scheme based on additive color mixing. *Pattern Recognition*, *41*(10), 3114–3129. doi:10.1016/j.patcog.2008.03.031

Yang, C. N., & Chung, T. H. (2010). A general multi-secret visual cryptography scheme. *Optics Communications*, *283*(24), 4949–4962. doi:10.1016/j.optcom.2010.07.051

Zhou, Z., Arce, R. G., Crescenzo, D. G., (2006) Halftone Visual Cryptography. *IEE transactions on image processing, 15*(8), 2441- 2453.