A new secure transmission scheme between senders and receivers using HVCHC without any loss

Saad Almutairi[1], Manimurugan S[2]* and Majed Aborokbah[1]

Abstract

This paper presents a novel secure medical image transmission scheme using hybrid visual cryptography and Hill cipher (HVCHC) between sender and receiver. The gray scale medical images have been considered as a secret image and split into different shares by visual cryptography (VC) encryption process. The split shares are once again encoded by Hill cipher (HC) encode process for improving the efficiency of the proposed method. In this process, the encrypted medical image (shares) pixels are converted as characters based on the character determination (CD) and lookup tables. In result, a secret image is converted into characters. These characters are sent to the receiver/authenticated person for the reconstruction process. In receiver side, the ciphertext has been decoded by HC decode process for reconstructing the shares. The reconstructed shares are decrypted by the VC decryption process for retaining the original secret medical image. The proposed algorithm has provided better CC, less execution time, higher confidentiality, integrity, and authentication (CIA). Therefore, using this proposed method, cent percent of the original secret medical image can be obtained and the secret image can be prevented from the interception of intruders/third parties.

Keywords: Transmission, Visual cryptography, Hill cipher, Medical images, Character conversion

1 Introduction

Cryptography is a method which is used to convert an original message into cipher message. There are many cryptographic methods available for encrypting the pain information/text. However, in this paper, we have used two foremost cryptography techniques of visual cryptography (VC) and Hill cipher (HC). VC is one of the powerful cryptosystems which converts a secret image into different secret shares. It was invented/proposed by Naor and Shamir [1] in 1994. The advantage of this system is that, while seeing the shares, original information cannot be identified and during decryption process, all shares must be presented. HC is also one of the cryptography methods; the original information is converted to characters [2, 3]. In 1929, it was introduced by Hill. We can define it in another way that a system of cryptography in which the plaintext is divided into sets of 'n' numbers of

letters, each of which is replaced by a set of 'n' number of cipher letters, is called a polygraphic system.

Zhuhong Shao, YuanyuanShang, RuiZeng, Huazhong-Shu, GouenouCoatrieux, and Jiasong Wu had introduced a novel robust watermarking scheme color image copyright protection. This scheme is based on the VC and quaternion-type moment invariants. They used VC for constructing the ownership share. Later, the ownership share is registered and it is responsible for authentication. In result, their proposed scheme provides a better robustness against different attacks [4]. S. Cimato, R. De Prisco, and A. De Santis had introduced a (k, n) colored-black-and-white visual cryptography scheme (CBW-VCS), which adopts colored pixels in shadow images to share a black and white secret image [5–10]. In connection with the same, Ching-NungYang, Li-Zhe Sun, and Song-Ruei Cai proposed to extend conventional BW-EVCS to the CBW-EVCS. It has two main divisions, one constructed (k, n)-CWB-EVCSs, and another one is that all constructions prove to satisfy security, contrast, and cover image conditions [11]. S

* Correspondence: smanimurugan@yahoo.co.in
[2]Department of Computer Engineering, Faculty of Computers and Information Technology, University of Tabuk, Tabuk, Saudi Arabia
Full list of author information is available at the end of the article

Manimurugan and Porkumaran introduced a novel encryption scheme based on the visual cryptography. In this proposed method, the given medical image had encrypted and compressed before the transmission. In result, they claimed that the proposed technique had provided double encryptions [12, 13].

In 2016, Tayebe Amiri and Mohsen Ebrahimi Moghaddam proposed VC-based watermarking scheme for multiple cover images. This scheme concealed watermarking without modifying the cover image. To develop the same, they used discrete wavelet transform (DWT), singular value decomposition (SVD), and scale invariant feature transform (SWIFT). In experimental results, they showed the method robustness versus various attacks, especially rotation and scaling [14]. Xuehu Yan, Shen Wang, and Xiamu Niu had proposed a general threshold progressive visual secret sharing (PVSS) construction method from a case (2, n) with unexpanded shares in 2016. This scheme had the feature of (k, n) threshold with no pixel expansion, which could be loss-tolerant and control access for a wider application. Based on the proposed construction method, a new threshold PVSS scheme was constructed. They claimed that the proposed method performance was superior to relative approaches [15]. In 2016, Guangyu Wang, Feng Liu, and Wei Qi Yan had conducted an experiment embedding Braille into grayscale and halftone images as well as VC shares. The result indicated that the embedding of Braille had a little impact on VC secret revealing and enhances the security of VC shares [16]. S Manimurugan and his teammates presented various visual cryptography techniques related to the secure image transmission without the pixel expansions [17–21]. They achieved the good signal ratios of the reconstructed image.

A.V.N. Krishna and K. Madhuravani in 2012 introduced a modified Hill cipher using randomized approach. In this proposed technique, the plain text is divided into equal sized blocks. The output of hill cipher is randomized to generate multiple ciphertexts for one plain text [22]. In 2013, Suman Chandrasekhar, Akash H.P, Adarsh.K, and Smitha Sasi implemented a second level (advanced Hill cipher) of encryption using permutation approach, which made the cipher highly secure. This encryption scheme is highly reliable as it uses tamper detection of the ciphertext ensuring successful decryption of the cipher [23]. M. Nordin A. Rahman et al. all proposed a robust Hill algorithm (Hill++). The algorithm was an extension of the Affine Hill cipher (AHC) [24]. A random matrix key was introduced as an extra key for encryption. Furthermore, an involuntary matrix key formulation was also implemented in the proposed algorithm.

D.C. Mishra, R.K. Sharma, Rakesh Ranjan, and M. Hanmandlu had introduced a cryptosystem using AHC for color images in the year of 2015. In this approach,

they considered multiplicative keys of AHC from SLn(Fq) domain and additive keys of AHC from Mn(Fq) domain, which provides exorbitant key space for the proposed system [25]. Bibhudendra Acharya and his teammates introduced a modified Hill cipher for solving the drawbacks of the conventional scheme by iterations and interlacing. They claimed that this approach performed well than the conventional Hill cipher [26]. Adinarayana Reddy K and his co-research workers had proposed a prime circulant matrix which have been shared as a secret key and a non-singular matrix G. It uses a public key such that the determinant of coefficient matrix Gc is zero [27]. In 2014, Neha Sharma and Sachin Chirgaiya had proposed a new variant of Hill cipher, to find the decryption of the ciphertext even when the key matrix was non-invertible [28].

In above statements, many authors had proved different image encryption techniques. However, each method has its own merits and demerits. This paper presents a novel secure medical image transmission scheme using hybrid visual cryptography and Hill cipher (HVCHC). The entire work has been divided into seven sections in this paper.

Section 1 discusses the literature review of conventional VC and HC. Sections 2 and 3 describe the proposed encryption and decryption techniques. Section 4 considers the experimental results and the conclusion is discussed in Section 5. Sections 6 and 7 deals with the acknowledgement and references.

2 Proposed HVCHC encryption process

The main aim of this proposed system is to provide a secure transmission to avoid hacker activities in telemedicine or public networks. In order to fulfill the same, this paper has introduced a HVCHC cryptographic system for medical image transmission. The proposed scheme of HVCHC encryption process is described in this section. It has been classified into four major divisions of sub-band creation, 8-bit conversion, permutation, and substitution processes as shown in Fig. 1.

The first three processes are based on the VC and substitution is based on the HC. The main advantage of this encryption process is that the medical image can be converted into ciphertext of characters; no pixel expansion was performed in VC. In order to ensure the integrity of the data, a header is created and pixels are swapped as much as possible within the image. The header contains ciphertext information.

2.1 Sub-band creation process

The grayscale medical image is considered as an input for this process. Initially, the given medical image $\sum_{i,j=0}^{m,n} M_{(i,j)}$ splits into 2×2 sub-bands. In result, four equal sub-bands of $\sum_{i,j=0}^{m/2,n/2} M_{(i,j)}, \sum_{i=1,\ j=\frac{n}{2}+1}^{\frac{m}{2},n} M_{(i,j)}, \sum_{i=\frac{m}{2}+1,j=1}^{m,\frac{n}{2}} M_{(i,j)}$,
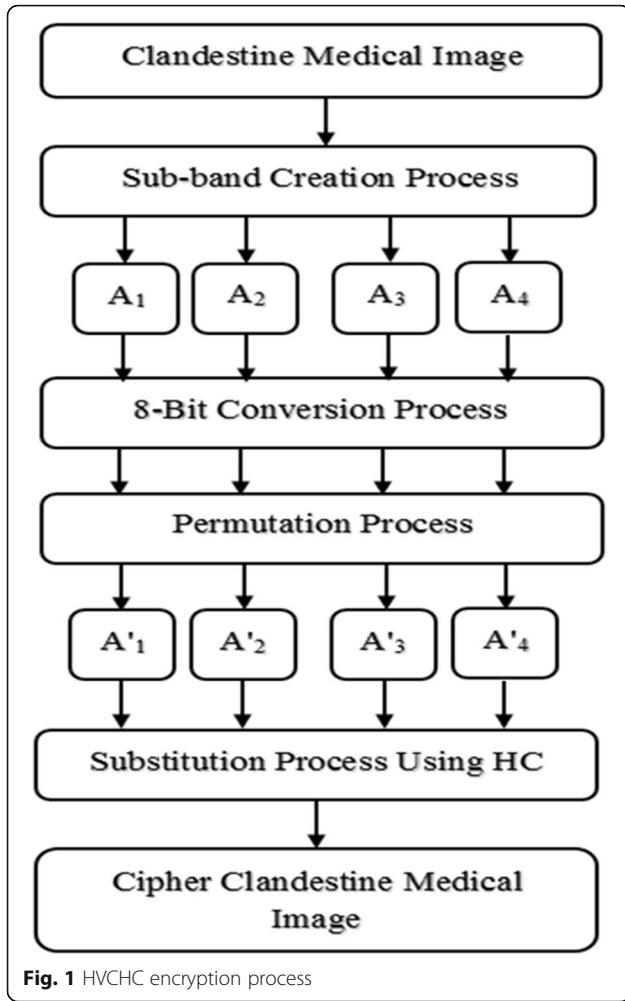
Fig. 1 HVCHC encryption process

and $\sum_{i=\frac{m}{2}+1,j=\frac{n}{2}+1}^{m,n} M_{(i,j)}$ can be obtained, in Eq. 1. Sub-band creation, 8-bit conversion, and permutation processes have an important role in order to generate the secret shares by VC. Equation 2 states the segregated sub-bands of A_1, A_2, A_3, and A_4.

$$\sum_{i,j=0}^{m,n} M_{(i,j)} = \sum_{i,j=0}^{m/2,n/2} M_{(i,j)} \oplus \sum_{i=1,j=\frac{n}{2}+1}^{\frac{m}{2},n} M_{(i,j)}$$
$$\oplus \sum_{i=\frac{m}{2}+1,j=1}^{m,\frac{n}{2}} M_{(i,j)} \oplus \sum_{i=\frac{m}{2}+1,j=\frac{n}{2}+1}^{m,n} M_{(i,j)} \quad (1)$$

$$\sum_{i,j=0}^{m,n} M_{(i,j)} = A_1 \oplus A_2 \oplus A_3 \oplus A_4 \quad (2)$$

There are certain reasons why this process has been incorporated. When the image splits into various sub-bands, it is easy to swap the pixels/interchange the pixel's position as much as possible within the image. On the other hand, the complexity of the algorithm is improved.

2.2 8-Bit conversion process

The second process of HVCHC is 8-bit conversion process. In this process, every segregated sub-band pixels are converted into 8-bit binary value $\sum_{n=1}^{\text{Max}} \text{Con}_{8\text{bit}} (A_n)$, the Max represents the maximum number of sub-bands. It has been illustrated in Eq. 3. In result A_1', A_2', A_3', and A_4' sub-bands are generated from the conversion process.

$$\sum_{n=1}^{\text{Max}} \text{Con}_{8\text{bit}} (A_n) = \sum_{n=1}^{1} \text{Con}_{8\text{bit}} (A_n) + \sum_{n=2}^{2} \text{Con}_{8\text{bit}} (A_n)$$
$$+ \sum_{n=3}^{3} \text{Con}_{8\text{bit}} (A_n) + \sum_{n=4}^{4} \text{Con}_{8\text{bit}} (A_n) \quad (3)$$

$$\sum_{n=1}^{\text{Max}} \text{Con}_{8\text{bit}} (A_n) = A_1' \oplus A_2' \oplus A_3' \oplus A_4' \quad (4)$$

2.3 Permutation process

The third process is permutation process. There are five different levels in this process. In level-1, every binary sub-bands A_1', A_2', A_3', and A_4' bits are separated based on an odd and even positions, illustrated in Fig. 3 and Eq. 5. The $\sum_{i,j=1}^{m,n} A_1'$ is segregated into odd positioned bits $\sum_{i,j=1}^{m,n} B_1$ and even positioned bits $\sum_{i,j=1}^{m,n} B_2$.

Similarly, $\sum_{i,j=1}^{m,n} A_2'$ is divided into $\sum_{i,j=1}^{m,n} B_3$ and $\sum_{i,j=1}^{m,n} B_4$; $\sum_{i,j=1}^{m,n} A_3'$ is divided into $\sum_{i,j=1}^{m,n} B_5$ and $\sum_{i,j=1}^{m,n} B_6$; $\sum_{i,j=1}^{m,n} A_4'$ is divided into $\sum_{i,j=1}^{m,n} B_7$ and $\sum_{i,j=1}^{m,n} B_8$.

Table 1 Character determination table

0	1	2	3	4	5	6	7	8	9	10	11	12
Z	Y	X	W	V	U	T	S	R	Q	P	O	N
13	14	15	16	17	18	19	20	21	22	23	24	25
M	L	K	J	I	H	G	F	E	D	C	B	A

Table 2 Lookup table

0	1	2	3	4	5	6	7	8	9
A	B	C	D	E	F	G	H	I	J
10	11	12	13	14	15	16	17	18	19
K	L	M	N	O	P	Q	R	S	T
20	21	22	23	24	25	00	01	02	03
U	V	W	X	Y	Z	A	B	C	D
04	05	06	07	08	09				
E	F	G	H	I	J				

$$\sum_{i,j=1}^{m,n} A'_1 \oplus \sum_{i,j=1}^{m,n} A'_2 \oplus \sum_{i,j=1}^{m,n} A'_3 \oplus \sum_{i,j=1}^{m,n} A'_4 = \left[\sum_{i,j=1}^{m,n} B_1 \right.$$

$$+ \sum_{i,j=1}^{m,n} B_2] \oplus \left[\sum_{i,j=1}^{m,n} B_3 + \sum_{i,j=1}^{m,n} B_4 \right] \oplus \left[\sum_{i,j=1}^{m,n} B_5 \right.$$

$$\left. + \sum_{i,j=1}^{m,n} B_6 \right] \oplus \left[\sum_{i,j=1}^{m,n} B_7 + \sum_{i,j=1}^{m,n} B_8 \right]$$

$$(5)$$

In level-2, the odd sub-bands of $\sum_{i,j=1}^{m,n} B_1$, $\sum_{i,j=1}^{m,n} B_3$, $\sum_{i,j=1}^{m,n} B_5$, and $\sum_{i,j=1}^{m,n} B_7$ are combined as $\sum_{i,j=1}^{m,n} C_1$ and an even sub-bands of $\sum_{i,j=1}^{m,n} B_2$, $\sum_{i,j=1}^{m,n} B_4$, $\sum_{i,j=1}^{m,n} B_6$, and $\sum_{i,j=1}^{m,n} B_8$ are combined as $\sum_{i,j=1}^{m,n} C_2$ in Eqs. 6 and 7. In level-3, $\sum_{i,j=1}^{m,n} C_1$ and $\sum_{i,j=1}^{m,n} C_2$ are once again separated based on an odd and even positions $\sum_{i,j=1}^{m,n} D_1$, $\sum_{i,j=1}^{m,n} D_2$, $\sum_{i,j=1}^{m,n} D_3$, and $\sum_{i,j=1}^{m,n} D_4$ in Eqs. 8 and 9.

$$\sum_{i,j=1}^{m,n} B_1 \oplus \sum_{i,j=1}^{m,n} B_3 \oplus \sum_{i,j=1}^{m,n} B_5 \oplus \sum_{i,j=1}^{m,n} B_7 = \sum_{i,j=1}^{m,n} C_1$$

$$(6)$$

$$\sum_{i,j=1}^{m,n} B_2 \oplus \sum_{i,j=1}^{m,n} B_4 \oplus \sum_{i,j=1}^{m,n} B_6 \oplus \sum_{i,j=1}^{m,n} B_8 = \sum_{i,j=1}^{m,n} C_2$$

$$(7)$$

$$\sum_{i,j=1}^{m,n} C_1 = \left[\sum_{i,j=1}^{m,n} D_1 + \sum_{i,j=1}^{m,n} D_2 \right]$$

$$(8)$$

$$\sum_{i,j=1}^{m,n} C_2 = \left[\sum_{i,j=1}^{m,n} D_3 + \sum_{i,j=1}^{m,n} D_4 \right]$$

$$(9)$$

In level-4, the above sub-bands are merged based on odd and even. $\sum_{i,j=1}^{m,n} D_1$ and $\sum_{i,j=1}^{m,n} D_3$ are combined as $\sum_{i,j=1}^{m,n} E_1$. Likewise, $\sum_{i,j=1}^{m,n} D_2$ and $\sum_{i,j=1}^{m,n} D_4$ are combined as $\sum_{i,j=1}^{m,n} E_2$. Finally, $\sum_{i,j=1}^{m,n} E_1$ and $\sum_{i,j=1}^{m,n} E_2$ are combined as a single sub-band $\sum_{i,j=1}^{m,n} P$ in level-5. After these steps, in $\sum_{i,j=1}^{m,n} P$ every 8-bits are converted into corresponding decimal value $\sum_{n=1}^{Max} Con_{b2D} (P_n)$. In result, all binary subbands are converted into single secret share $Per_{(i,j)}$. These secret share pixels vary from 0 to 255, given in Eqs. 10–13.

$$\sum_{i,j=1}^{m,n} D_1 \oplus \sum_{i,j=1}^{m,n} D_3 = \sum_{i,j=1}^{m,n} E_1 \qquad (10)$$

$$\sum_{i,j=1}^{m,n} D_2 \oplus \sum_{i,j=1}^{m,n} D_4 = \sum_{i,j=1}^{m,n} E_2 \qquad (11)$$

$$\sum_{i,j=1}^{m,n} E_1 \oplus \sum_{i,j=1}^{m,n} E_2 = \sum_{i,j=1}^{m,n} P \qquad (12)$$
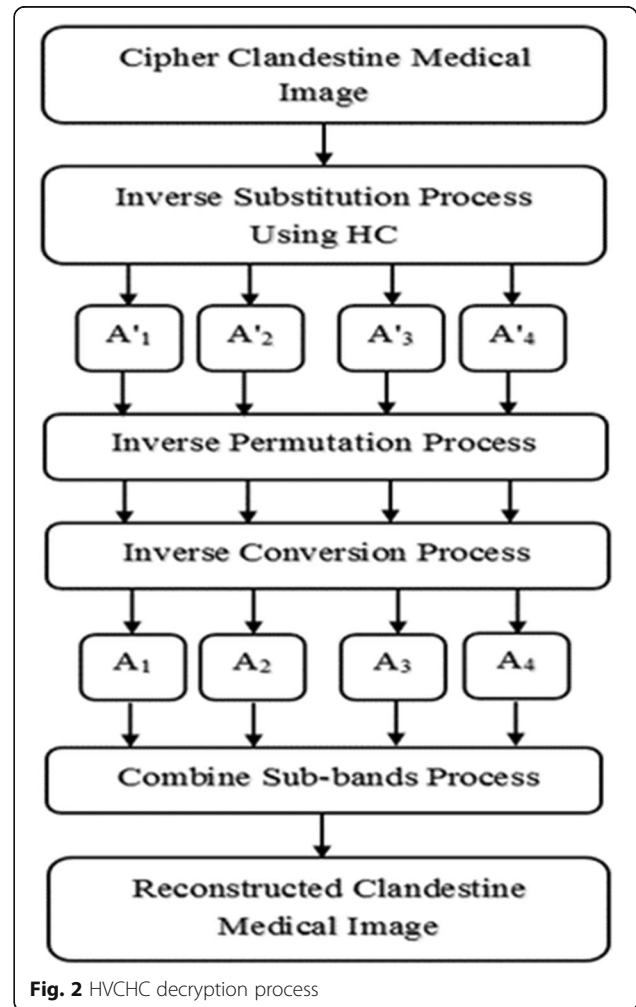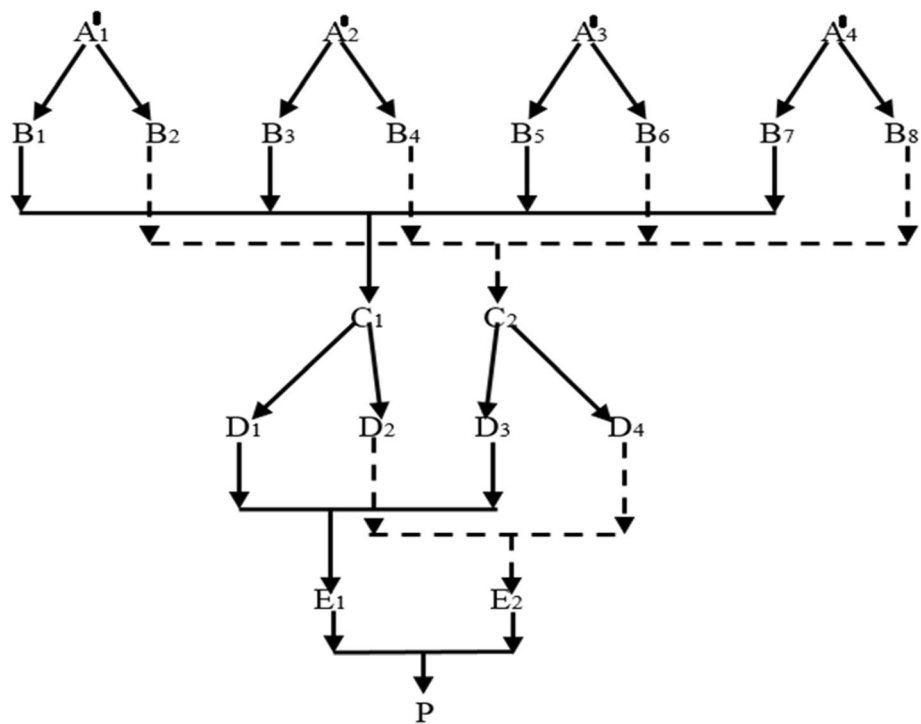

Fig. 2 HVCHC decryption process
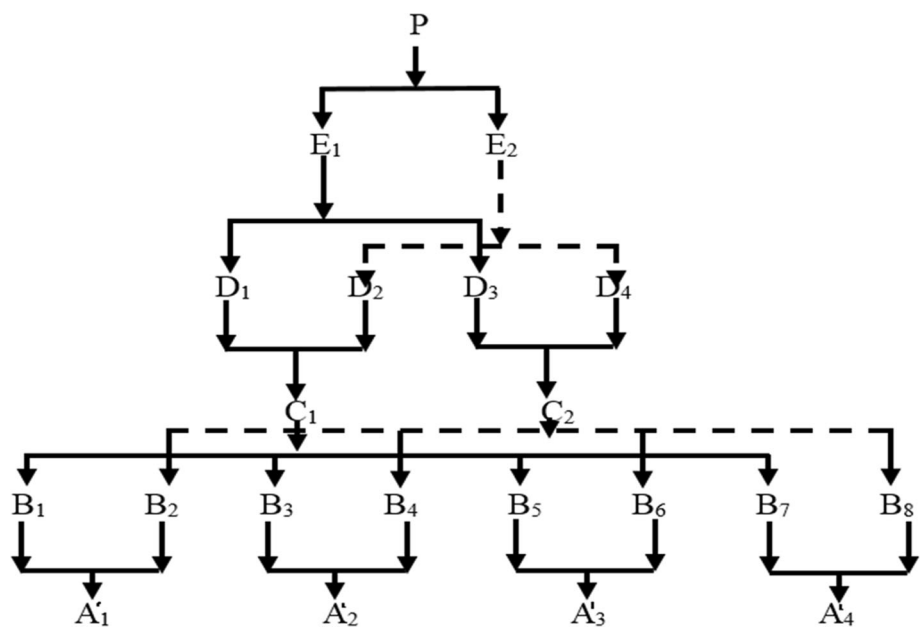
Fig. 3 HVCHC permutation process

Fig. 4 HVCHC inverse permutation process

$$\sum_{n=1}^{Max} Con_{b2D}\,(P_n) = Per_{(i,j)} \qquad (13)$$

Due to the substitution process of HC, the different secret shares are combined as single share. The main advantage of this process is that every sub-bands pixel is converted as binary bits and the same bits are interchanged as much as possible within the image.

Finally, after the swapping process, every 8-bits are converted into corresponding decimal value. This process clearly states that the every pixel is encrypted without loss and pixel expansion. To improve the proposed scheme strength and complexity of the single secret share, $\sum_{i,j=1}^{m,n} P$ is encoded by substitution process of HC.
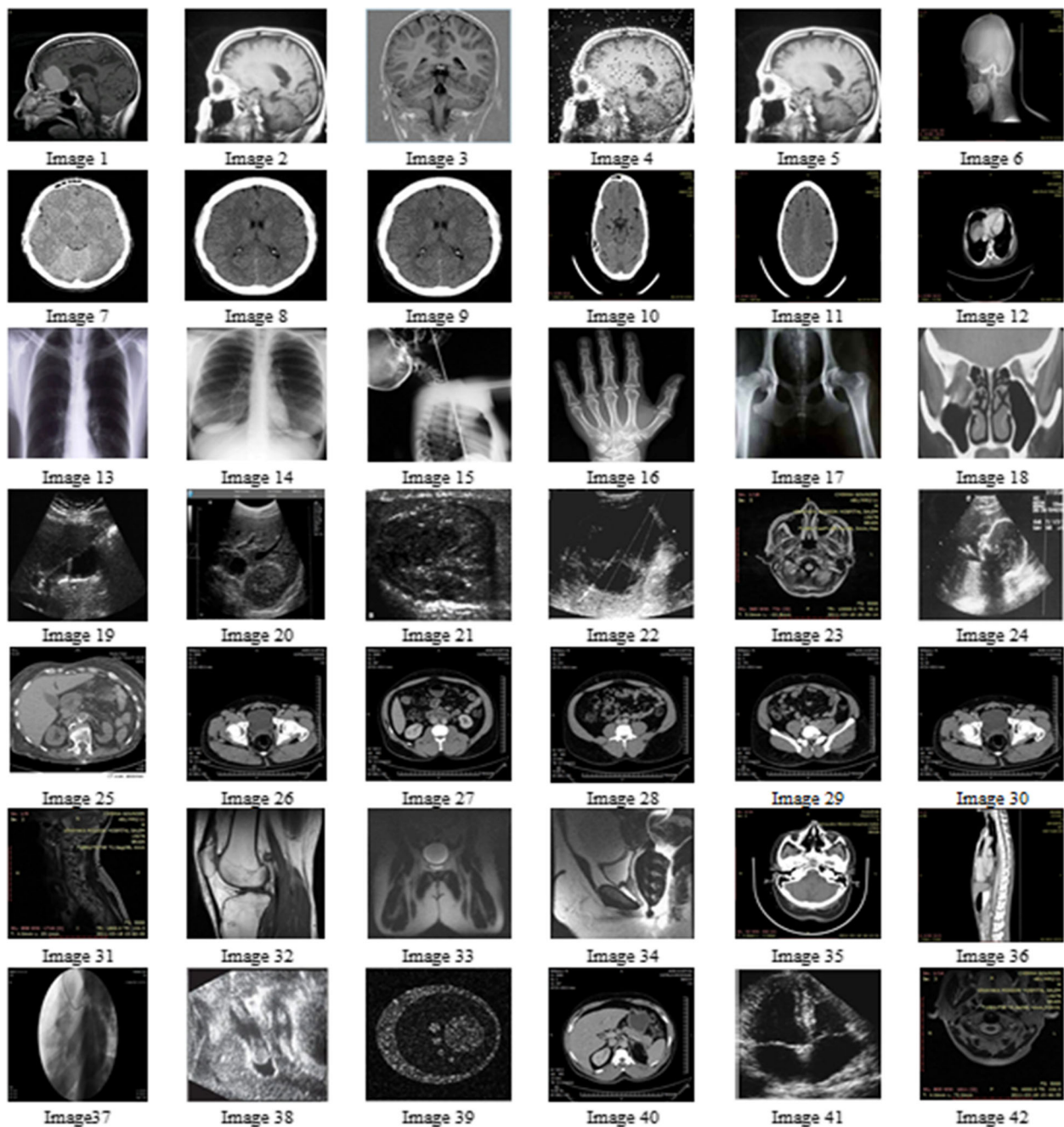

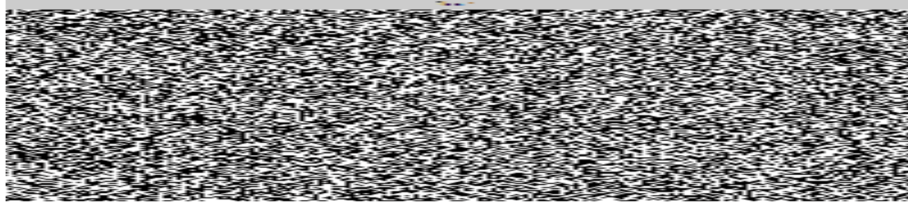**Fig. 5** Input gray scale medical images

Fig. 6 Output of the proposed VC scheme

2.4 Substitution process

$\sum_{i,j=1}^{m,n} \text{Per}$ pixels are replaced by alphabet characters based on the character determination (CD) table, given in Table 1 and Eq. 14. The HC substitution process is a symmetric encryption technique, where the secret letters are encrypted into ciphers. It is also called a polygraphic system. In this process, the character information $\sum_{i,j=1}^{m,n} c(\text{Per})$ is converted into encoded information (cipher character) with the support of Table 2.

In next step, the generated characters are encoded by proposed encode process as given in Eq. 15. In this process, $\sum_{i,j=1}^{m,n} e$ text is considered as a secret text S.

The secret text S is encrypted as a ciphertext C using an encryption key κ_e in Eq. 15. After the substitution process, the ciphertext $\sum_{i,j=1}^{m,n} C$ is sent along with the encryption key κ_e to the other end/authenticated person

for the decryption process. The complete computation for creating the ciphertext is computed by Eq. 15.

$$N2C\left[\sum_{i,j=1}^{m,n} \text{Per}\right] = \sum_{i,j=1}^{m,n} e \tag{14}$$

$$\sum_{i,j=1}^{m,n} C = [\kappa_e \times S] \mod 26 \tag{15}$$

2.5 Header 'H' creation

In this process, a header H is created. This H contains ciphertext information and substitution key; it can be used to ensure the integrity of the reconstructed secret image. After the encryption process, H along with ciphertext is sent to the receiver/authenticated person for reconstruction process in Eq. 16.

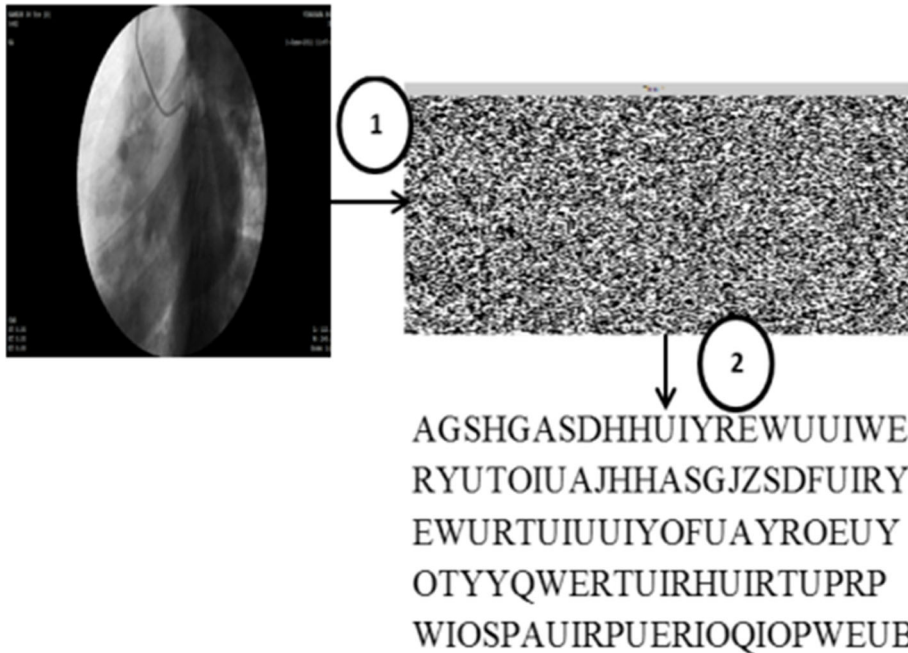$$\sum_{i,j=1}^{m,n} C + H = \text{Cipher} \tag{16}$$

Fig. 7 Steps 1 and 2 of HVCHC

3 HVCHC decryption process

Receiver/authenticated person receives a 'Cipher' from the sender. This 'Cipher' is segregated into $\sum_{i,j=1}^{m,n} C$ and H. To decrypt the ciphertext of $\sum_{i,j=1}^{m,n} C$, inverse substitution, inverse permutation, inverse conversion, and combine-sub-bands processes have crucial roles, illustrated in Fig. 2.

The HVCHC decryption process can be classified into two major divisions, one is based on the HC decode process and another one is based on VC decryption. The inverse substitution is designed based on the HC decode. The inverse permutation, inverse conversion, and combine sub-bands processes are based on VC decryption process. The merit of this process is that the pixel expansion is not performed, so the exact replica of the original image can be retrieved. However, the integrity is also measured after the reconstruction using a H (Fig. 3).

3.1 Inverse substitution process

The received ciphertext of $\sum_{i,j=1}^{m,n} C$ and encryption key κ_e are used for the decryption process. In this process, κ_e^{-1} and the determinant of κ_e are computed from the encryption key κ_e in Eqs. 17–19. The D denotes the determinant of κ_e. To find the decryption key κ_d, the computational value B is calculated from Eqs. 20 and 21. Using κ_d and $\sum_{i,j=1}^{m,n} C$, the $\sum_{i,j=1}^{m,n} e$ is retrieved from Eq. 22.

$$\kappa_e = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \tag{17}$$

$$\kappa_e^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \tag{18}$$
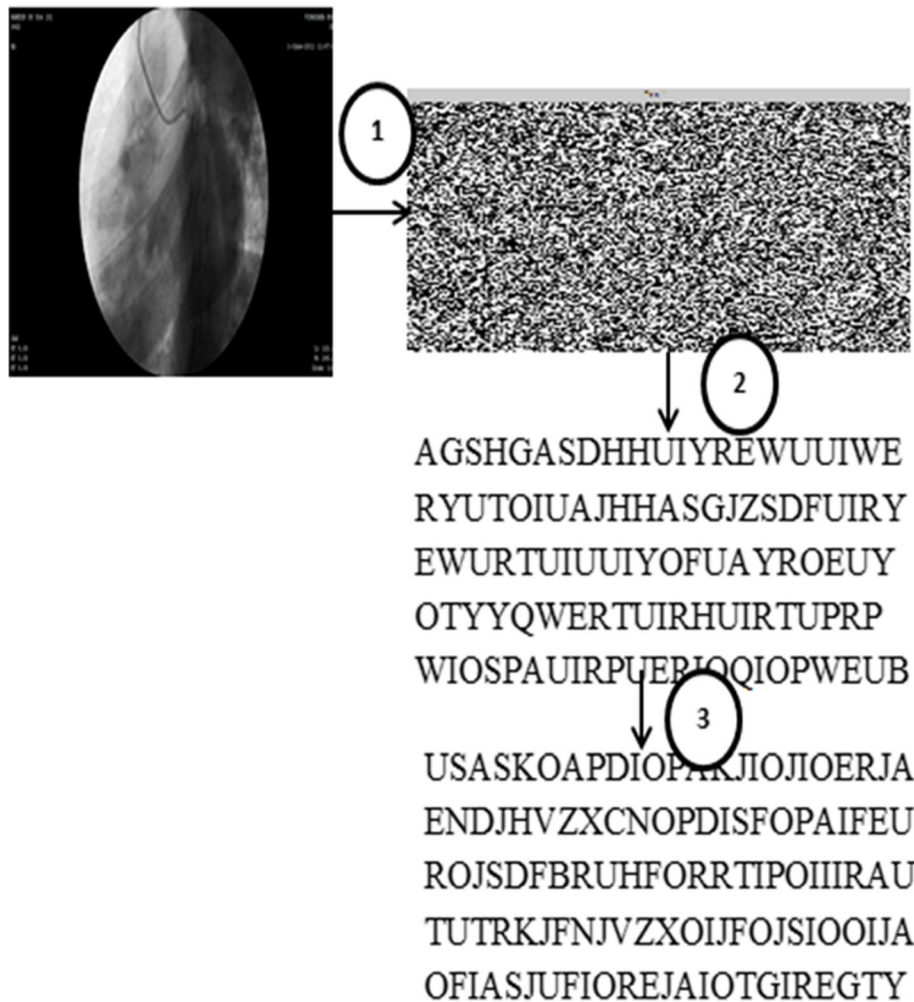
$$D = |k_e| = (ad-bc) \tag{19}$$

Fig. 8 Steps 1, 2, and 3 of HVCHC

$$D \times B = 1 \ \ \mathrm{mod} \ 26 \tag{20}$$

$$k_d = B\left[k_e^{-1}\right] \ \ \mathrm{mod} \ 26 \tag{21}$$

Finally, the inverse characters are converted into numbers based on the Table 1. In result, the $\sum_{i,j=1}^{m,n} \mathrm{Per}$ can be obtained from the Eq. 23.

$$\sum_{i,j=1}^{m,n} e = [k_d \times C] \ \ \mathrm{mod} \ 26 \tag{22}$$

$$C2N\left[\sum_{i,j=1}^{m,n} e\right] = \sum_{i,j=1}^{m,n} \mathrm{Per} \tag{23}$$

3.2 Inverse permutation process

This process is a reverse process of permutation process. In this process, every pixel in the obtained result of $\mathrm{Per}_{(i,j)}$ (inverse substitute process) is converted into 8-bit binary $\mathrm{Con}_{D2b} \ \mathrm{Per}_{(i,j)}$ in Eq. 24. In order to retrieve the A_1', A_2', A_3', and A_4', inverse process has been done from Eq. 5 to 12 in reverse order (equations from 12 to 5). The main aim of this process is that perfect replacement of the pixels back into their position and this is one of the main advantages. After the abovementioned computations, the A_1', A_2', A_3', and A_4' can be obtained. These

sub-bands are considered as an input for the inverse conversion process in Fig. 4.

$$\sum_{n=1}^{\mathrm{Max}} \mathrm{Con}_{D2b} \ \mathrm{Per}_{(i,j)} = \sum_{i,j=1}^{m,n} P \tag{24}$$

3.3 Inverse conversion process

In an inverse conversion process, every 8-bit binary values are converted into the corresponding decimal value. Equations 25 and 26 represent the computation of binary to decimal conversion.

$$\sum_{n=1}^{\mathrm{Max}} \mathrm{Con}_{8bit2D} \left(A_n'\right) = A_1' \oplus A_2' \oplus A_3' \oplus A_4' \tag{25}$$

$$\sum_{n=1}^{\mathrm{Max}} \mathrm{Con}_{Dec} \left(A_n\right) = \sum_{n=1}^{1} \mathrm{Con}_{Dec} \left(A_n'\right) + \sum_{n=2}^{2} \mathrm{Con}_{Dec} \left(A_n'\right)$$
$$+ \sum_{n=3}^{3} \mathrm{Con}_{Dec} \left(A_n'\right) + \sum_{n=4}^{4} \mathrm{Con}_{Dec} \left(A_n'\right) \tag{26}$$
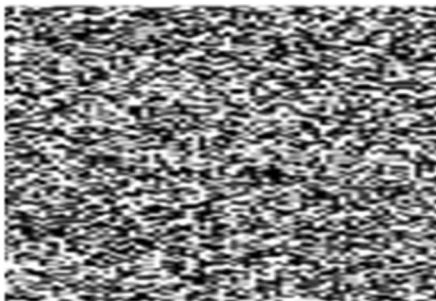
In these computations, $'\mathrm{Max}'$ denotes the maximum number of the sub-bands. In this proposed scheme, the maximum sub-bands are four. This decision/constraint is made to minimize the computation time in both sides of the sender and receiver. In result, the segregated sub-bands can be retrieved in Eq. 27.
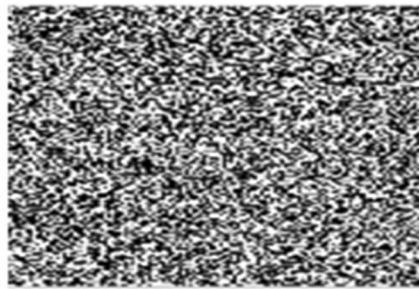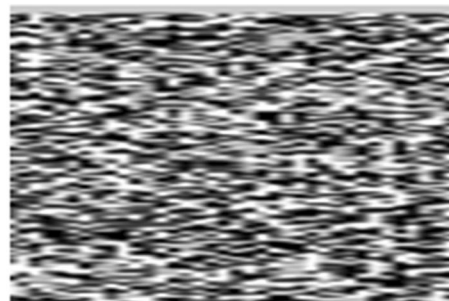

Fig. 9 Enlarged images in different angle

3.4 Combine sub-bands process

The combine subbands process is an inverse process of the split sub-bands process (Section 2.1). The obtained different sub-bands of inverse permutation process A_1, A_2, A_3, and A_4 are merged together as an image in Eq. 27. In result, the reconstructed medical image can be retrieved. Finally, the constructed image has been considered for the pixel by pixel analysis in an integrity check to ensure that the exact replica of the image is reconstructed or not. In this checking, 'H' has a vital role.

$$\sum_{n=1}^{Max} \text{Con}_{Dec}(A_n) = A_1 \oplus A_2 \oplus A_3 \oplus A_4 = \sum_{i,j=0}^{m,n} M_{(i,j)} \tag{27}$$

4 Experimental and result discussion

This section discusses the various experimental results of proposed and conventional system. Saad Al-Mutairi

and S Manimurugan had implemented the clandestine image transmission scheme to prevent from the intruders in 2016 and 2017. In this paper [18, 19], three encryption methods are considered (VC, steganography, and HC) for the secure transmission of the image.

However, to have a better encryption system in this proposed work, I have combined the two foremost encryptions of VC and HC. The previous work [18, 19] was considered as a conventional method. The difference between the conventional method and the proposed method is that the permutation and substitution steps are entirely different. Another important point of the proposed system is that it overcomes the existing method's limitations in an efficient manner.

In this experimentation, we have demonstrated nearly 1000 medical images. Though for this documentation, we have included 25 Gy scale medical images as shown in Fig. 5. It includes computed tomography (CT), magnetic resonance imaging (MRI), X-ray, ultrasound (US),

Table 3 Proposed and conventional encryption methods performances

| Images	Size (KB)	Encrypted size (KB)		Time (s)				Reconstructed size(kb)		CC		Error rate (MSE)		Pixel expansion	
				Encry		Decry									
		Conv.	Prop.	Conv.	Prop.	Conv.	Prop.	Conv.	Prop.	Conv.	Prop.	Conv.	Prop.	Conv.	Prop.
1.	256	312	201	10.26	4.45	9.52	4.00	255.60	256	0.99	1.0	0.01	0.00	No	No
2.	256	345	196	11.20	4.26	9.26	4.12	255.30	256	0.99	1.0	0.01	0.00	No	No
3.	256	362	235	10.33	4.44	9.26	4.14	254.30	256	0.98	1.0	0.02	0.00	No	No
4.	256	386	221	10.56	5.12	9.35	4.59	255.10	256	0.99	1.0	0.01	0.00	No	No
5.	256	374	220	10.12	4.53	9.17	4.10	255.20	256	0.99	1.0	0.01	0.00	No	No
6.	256	325	218	09.53	4.42	9.28	4.21	255.40	256	0.99	1.0	0.01	0.00	No	No
7.	256	368	205	12.05	4.35	9.18	4.02	255.02	256	0.99	1.0	0.01	0.00	No	No
8.	256	314	193	12.36	4.31	9.36	4.05	255.12	256	0.99	1.0	0.01	0.00	No	No
9.	256	356	197	11.59	4.23	10.02	4.02	255.80	256	0.99	1.0	0.01	0.00	No	No
10.	256	355	204	10.54	5.01	9.01	4.56	255.06	256	0.99	1.0	0.01	0.00	No	No
11.	256	348	189	10.26	5.23	9.45	5.01	255.02	256	0.99	1.0	0.01	0.00	No	No
12.	256	366	196	11.02	4.21	10.03	4.13	255.09	256	0.99	1.0	0.01	0.00	No	No
13.	256	368	215	11.20	5.06	8.59	4.36	255.16	256	0.99	1.0	0.01	0.00	No	No
14.	256	374	211	10.37	4.29	9.02	3.50	255.02	256	0.99	1.0	0.01	0.00	No	No
15.	256	381	204	10.34	5.36	9.07	4.59	255.05	256	0.99	1.0	0.01	0.00	No	No
16.	256	392	193	12.33	4.02	9.06	3.45	255.23	256	0.99	1.0	0.01	0.00	No	No
17.	256	358	201	11.25	4.35	9.15	4.01	255.45	256	0.99	1.0	0.01	0.00	No	No
18.	256	359	200	11.46	5.22	9.17	5.12	255.02	256	0.99	1.0	0.01	0.00	No	No
19.	256	356	193	12.38	4.35	9.04	3.59	255.02	256	0.99	1.0	0.01	0.00	No	No
20.	256	369	209	12.02	4.12	9.37	3.45	255.31	256	0.99	1.0	0.01	0.00	No	No
21.	256	344	210	11.45	4.09	9.21	3.40	255.78	256	0.99	1.0	0.01	0.00	No	No
22.	256	389	215	10.25	4.39	9.25	4.16	255.24	256	0.99	1.0	0.01	0.00	No	No
23.	256	354	198	11.26	5.02	9.64	4.52	255.14	256	0.99	1.0	0.01	0.00	No	No
24.	256	356	193	12.50	4.06	9.20	4.42	254.98	256	0.98	1.0	0.02	0.00	No	No
25.	256	326	190	12.03	5.02	9.50	4.31	255.12	256	0.99	1.0	0.01	0.00	No	No
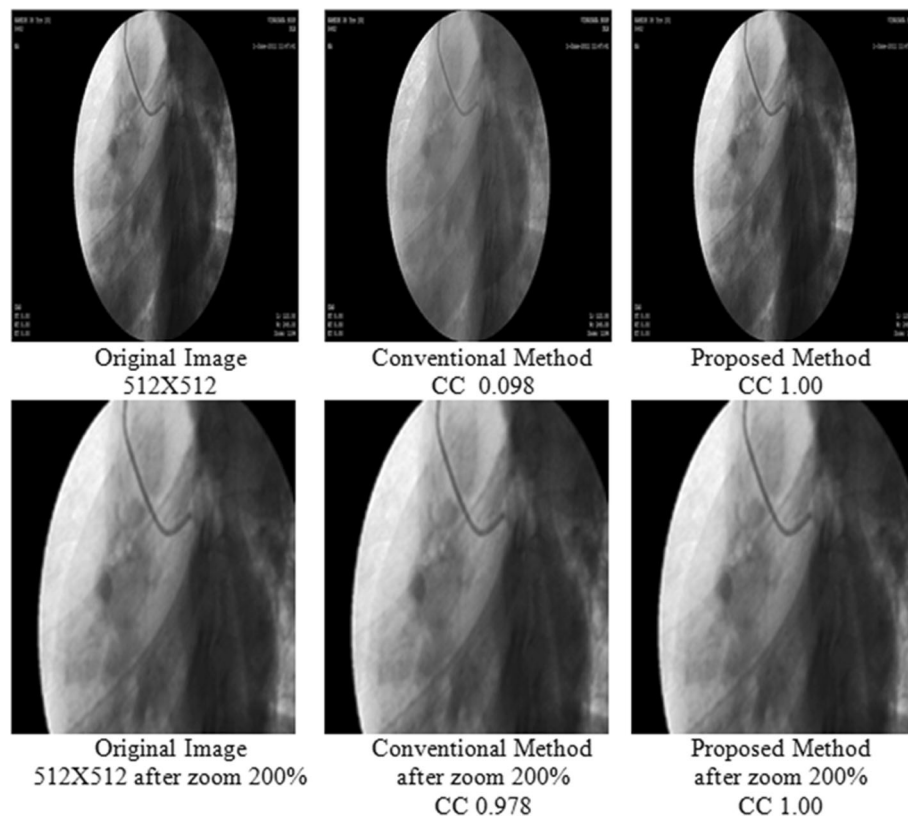
Fig. 10 Comparison of conventional and proposed reconstruction image quality

etc. The conventional and proposed methods are coded in MATLAB software.

All input images are 512×512 dimensions, .BMP format, and 256 kb size. Basically, some of the medical images are in. DICOM (digital imaging and communications in medicine) format; however, we have converted. DICOM into. BMP for this research work.

In this proposed system, the given input medical images are encrypted by VC scheme. The output of this VC scheme is illustrated in Fig. 6. In order to make an efficient system, the same output of the proposed VC is encoded by HC scheme. In this encode process, two different processes are incorporated.

The output image of proposed VC scheme is converted into a set of characters based on Table 1 and it
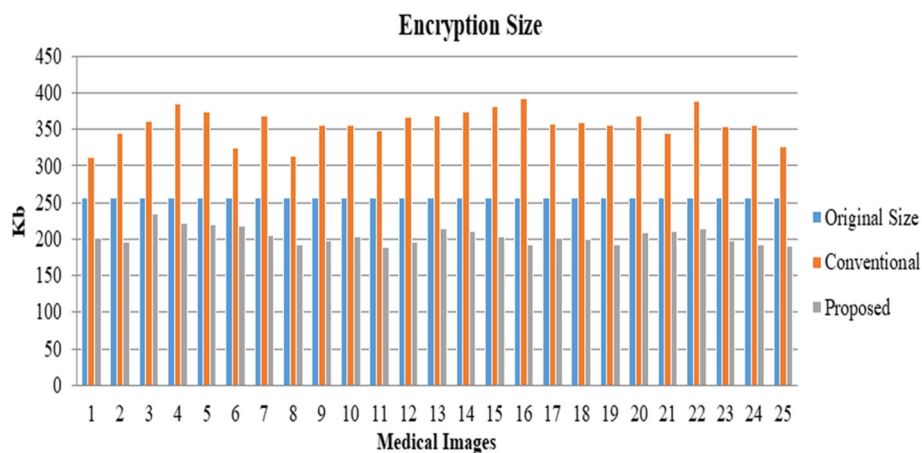

Fig. 11 Comparison of conventional and proposed schemes encryption size

has been illustrated in Fig. 7. In the second step, the converted characters are encoded by proposed HC scheme in Fig. 8.

In result, the given input of the medical image is converted into a set of characters. The main advantage of this character conversion is that two time's character conversions are performed in order to improve the confidentiality and strengthen the proposed scheme.

In addition to examine the confidentiality of the proposed scheme, we have made pixel analysis in every stage. In Fig. 9, it have been illustrated that there are different sizes of the enlarged images for identifying the original image. This enlarge process have been done in four angles 100, 150, 175, and 200 percentages. However, the proposed scheme provides the better performance. In the result, it is very hard to identify the original secret image. While converting the same into different steps of characters, the proposed scheme is provides the better performances. The significance of this proposed VC is that no pixel expansions have been performed.

Table 3 illustrates the proposed and convention schemes performances based on the different parameters of size, time, correlation coefficient (CC), mean squared error (MSE), and pixel expansion. The conventional scheme [18, 19] has been implemented and tested with the proposed system.

The main difference between the conventional scheme and proposed scheme is that the conventional scheme takes high execution time in both phases of encryption and decryption. In addition, the conventional method reconstructs the partially exact replica of the original image. In order to overcome the same, the proposed scheme has reconstructed an exact replica of the image. These achievements are due to the perfect framework of the proposed system. To achieve good medical image processing, the exact replica of the pixels must be

reconstructed. In case of any loss during the reconstruction process, the reconstructed medical image is not useful for further activities. Keeping this point in mind, the proposed scheme has been designed. The error rate is very minimal than the conventional system. Another important point is that both the methods have no pixel expansion.

While comparing with the encryption and decryption size, the proposed scheme provides a superior result than the conventional. Figure 10 states the reconstruction performance of both the conventional and the proposed system. The reconstructed image quality is not measured by (peak signal-to-noise ratio (PSNR). Instead of PSNR, pixel by pixel analysis of CC has been taken. In result, the conventional method has performed good results between 0.98 to 0.99. When the CC value is exactly one, the reconstructed image pixels are exactly presented. The proposed scheme provides the exact copy of all images. It means that the exact replica of the image has been reconstructed by the proposed scheme.

This scheme is mainly designed for the medical images. In Fig. 10, the conventional method reconstructed nearly exact replica of the image, due to the CC value of 0.98. It means there is a loss in the pixel during the process time. On the other hand, the proposed scheme has obtained the CC value exactly one. It proves that the proposed scheme has retrieved the exact replica of the original image. To make a better analysis report, the CC has been measured after enlarging the image. The results are given in the second row of Fig. 10.

Figure 11 states the comparison of encryption size with conventional and proposed schemes. In this comparison, the proposed method obtained the less encryption size than the original size. It is due to the double character conversion. The convention method obtained the higher size than the original image size. This difference occurred is due to the VC and character conversion
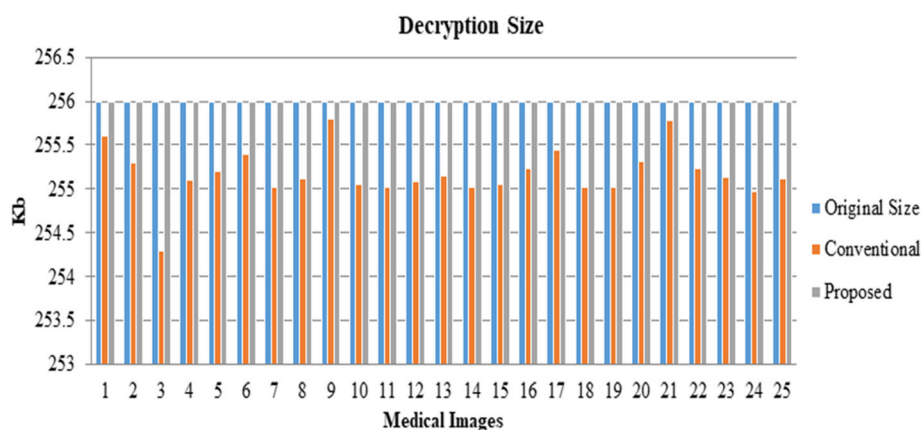

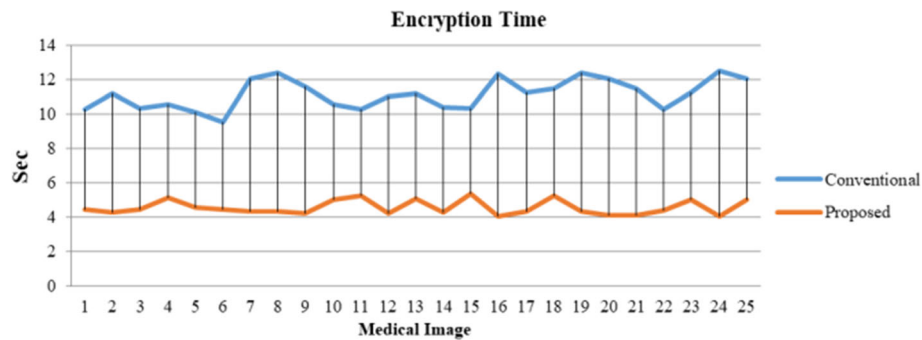**Fig. 12** Comparison of conventional and proposed schemes decryption size

Fig. 13 Comparison of conventional and proposed schemes encryption time

processes. In Fig. 12, both proposed and conventional methods decryption sizes are defined.

Both methods provide the better performance. However, the conventional method reconstructs the partially exact replica of the original image. But the proposed scheme reconstructs the exact replica of the image. In Figs. 13 and 14, the encryption and decryption times are denoted. The proposed system provides the better execution time for encryption process compared to the conventional scheme. The time variations of proposed scheme are maximum 4 to 5 s.

Similarly, the conventional scheme time variations are between 9 and 12.5 s. In decryption process, the proposed scheme time variations are from 4 to 5 s and from 9 to 10 s by the conventional scheme.

In order to prove the algorithm complexity and strength, the pixels are swapped as much possible within the image itself. We have used different attacks for analysis the proposed scheme competency. In human visual attack, the proposed scheme has provided a good result and pixel by pixel analysis is also done. Therefore, the proposed scheme has obtained the magnificent results than other methods.

5 Conclusion

Many encryption algorithms have been proposed for images. However, this paper has proposed a different type of encryption for medical images without any loss of the pixels. In this paper, we have compared with the traditional (conventional) approach to prove the efficiency of the proposed HVCHC scheme. Many parameters are considered for the comparison. It has been given in the experimental section. In the result, the traditional method of triple encryption is performed well. Although, there are some improvements in the proposed HVCHC compared to the conventional method. One of the improvements is that it reduces the execution time as much as possible compared than the conventional method. An important point is that, while processing the medical image, the pixel loss should not occur. This point is also addressed in this proposed method. In result, perfect/exact replica of the original medical image can be retrieved. The conventional method has provided error rate between 1 and 2%, but the proposed method provides error rate as zero. To measure the quality of the image, PSNR is not considered, instead of that CC has been considered for pixel by pixel analysis. In addition, the proposed algorithm can reduce the size during the encryption process than original and conventional encryption size. The visual and pixel attacks are also done by the expert groups. In result, the proposed scheme
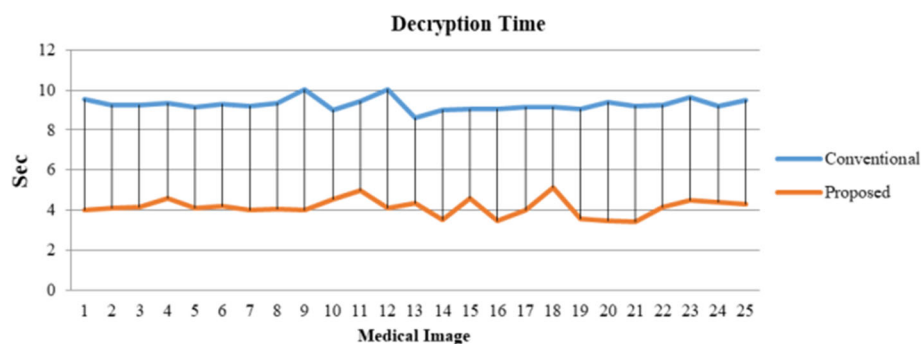

Fig. 14 Comparison of conventional and proposed schemes decryption time

defended visual and pixel by pixel attacks in an efficient manner than conventional method. Therefore, this proposed method of encryption provides double encryption, the minimum execution time of encryption and decryption, reduces the size from the original after the encryption process, 100% perfect reconstructions, provides better performance against hacker/third parties/attackers.

Abbreviations

AHC: Affine Hill cipher; CBW: VCS-colored-black-and-white visual cryptography scheme; CD: Character determination; CIA: Confidentiality, integrity, and authentication; CT: Computed tomography; DICOM: Digital imaging and communications in medicine; DWT: Discrete wavelet transform; HC: Hill cipher; HVCHC: Hybrid visual cryptography and Hill cipher; Kb: Kilobyte; MRI: Magnetic resonance imaging; SVD: Singular value decomposition; SWIFT: Scale invariant feature transform; US: Ultrasound; VC: Visual cryptography

About the authors

SAAD AL-MUTAIRI received the BSc from Al-Ahliyya Amman University, Jordon, the MSc and PhD degrees from De Montfort University, U.K. He is currently working as a Dean in Deanship of Information Technology, University of Tabuk, Saudi Arabia. His research interests are Software Engineering, Context Aware System, Cloud Computing, Cyber security, Steganography, etc. He has published ample of papers in international refereed journals and conferences in his research areas. He is a professional member in IEEE.

S.MANIMURUGAN has completed his Bachelor, Master and Ph.D in Computer Science and Engineering, Anna University, India. Currently, he is working in Computer Engineering, Faculty of Computers and Information Technology, University of Tabuk, Tabuk City, Saudi Arabia. His research areas are Image processing, Information Security, Visual Cryptography, IoT, and Steganography. He is a professional member in IEEE and a life Member of Indian Society for Technical Education (MISTE). He has published nearly 70+ research papers in several international and national forums which include various ISI, Clarivate analytics, Scopus, and IEEE indexed international conferences as well. He also has been a celebrated editor and reviewer for many international journals like Elsevier and springer and so on.

MAJED ABOROKBAH is a Dean in Faculty of Computers and Information Technology, University of Tabuk, Saudi Arabia. He received the BSc from Taif University, Saudi Arabia, the Msc from Bradford University, UK and the PhD degree from De Montfort University, U.K. His research is in the areas of Software Engineering, Context Aware System, Cyber security, Steganography, etc. He has published many papers in international journals and conferences, has organized various workshops and conferences in his research areas. He has established the robotics center in University of Tabuk.

Availability of data and materials

(Mandatory for Biology and Medical journals): We thank the Vinayaga mission Hospital, India for providing the sample image data for this research work. There is no issue if the data shares among the research community.

Authors' contributions

There are three authors that have completed this work in which SA has prepared the encryption section, SM has done the decryption section, and MA has completed the experimental and result sections. Finally, the entire paper is affirmed by all authors. All authors read and approved the final manuscript.

Competing interests

Yes.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Author details

[1]Department of Computer Science, Faculty of Computers and Information Technology, University of Tabuk, Tabuk, Saudi Arabia. [2]Department of Computer Engineering, Faculty of Computers and Information Technology, University of Tabuk, Tabuk, Saudi Arabia.

References

1. M. Naor, A. Shamir, *Visual cryptography, in: advances in cryptology, EUROCRYPT'94, in: LNCS*, vol 950 (1994), pp. 1–12.
2. L.S. Hill, Cryptography in an algebraic alphabet. Am. Math. Mon. **36**(6), 306–312 (1929).
3. L.S. Hill, Concerning certain linear transformation apparatus of cryptography. Am. Math. Mon. **38**, 135–154 (1931).
4. Z. Shao, Y. Shang, R. Zeng, H. Shu, G. Coatrieux, J. Wu, Robust watermarking scheme for color image based on quaternion-type moment invariants and visual cryptography. Signal Process. Image Commun. **48**, 12–21 (2016).
5. S. Cimato, R. De Prisco, A. De Santis, Optimal colored threshold visual cryptography schemes. Des. Codes Cryptography **35**, 311–335 (2005).
6. S. Cimato, R. De Prisco, A. De Santis, Probabilistic visual cryptography schemes. Comput. J. **49**, 97–107 (2006).
7. S. Cimato, A. De Santis, A.L. Ferrara, B. Masucci, Ideal contrast visual cryptography schemes with reversing. Inf. Process. Letter **93**, 199–206 (2005).
8. S. Cimato, R. De Prisco, A. De Santis, Colored visual cryptography without color darkening. Theor. Comput. Sci. **374**, 261–276 (2007).
9. S. Cimato, R. De Prisco, A. De Santis, *Visual cryptography for color images, in: visual cryptography and secret image sharing* (CRC Press, London, 2012), pp. 31–56 ISBN 978–1–4398-3721-4.
10. R. De Prisco, A. De Santis, Color visual cryptography schemes for black and white secret images. Theor. Comput. Sci. **510**, 62–86 (2013).
11. C.-N. Yang, L.-Z. Sun, S.-R. Cai, Extended color visual cryptography for black and white secret image. Theor. Comput. Sci. **609**, 143–161 (2016).
12. S. Manimurugan, K. Porkumaran, Secure medical image compression using block pixel Sort algorithm. Eur. J. Sci. Res. **56**(2), 129–138 (2011).
13. S. Manimurugan, K. Porkumaran, Fast and efficient secure medical image compression schemes. Eur. J. Sci Res **56**(2), 139–150 (2011).
14. T. Amiri, M.E. Moghaddam, A new visual cryptography based watermarking scheme using DWT and SIFT for multiple cover images. Multimed. Tools Appl. **75**, 8527–8543 (2016).
15. X. Yan, S. Wang, X. Niu, Threshold progressive visual cryptography construction with unexpanded shares. Multimed. Tools Appl. **75**, 8657–8674 (2016).
16. G. Wang, F. Liu, W.Q. Yan, Basic visual cryptography using braille. Int. J. Digit. Crime Forensics **8**(3), 85–93 (2016).
17. S. Manimurugan, C. Narmatha, Secure and efficient medical image transmission by new tailored visual cryptography scheme with LS compressions. Int. J. Digit. Crime Forensics **7**(1), 26–50 (2015).
18. S. Al-Mutairi, S. Manimurugan, An efficient secret image transmission scheme using Dho-encryption technique. Int. J. Comput. Sci. Inf. Secur **14**(10), 446–460 (2016).
19. S. Al-Mutairi, S. Manimurugan, The clandestine image transmission scheme to prevent from the intruders. Int. J. Adv. Appl. Sci. **4**(2), 52–60 (2017).
20. S. Manimurugan, K. Porkumaran, C. Narmatha, "The new block pixel Sort algorithm for TVC encrypted medical image", imaging science. Journal **62**(8), 403–414 (2014).
21. S. Manimurugan, C. Narmatha, K. Porkumaran, The new approach of visual cryptography scheme for protecting the grayscale medical images. J. Theor. Appl. Inf. Technol. **69**(3), 552–561 (2014).

22. A.V.N. Krishna, K. Madhuravani, A Modified Hill cipher using randomized approach. Int. J. Comput. Netw. Inf. Secur. **5**, 56–62 (2012).
23. A.H.P. Suman Chandrasekhar, K. Adarsh, S. Sasi, A secure encryption technique based on advanced Hill cipher for a public key cryptosystem. IOSR J. Comput. Eng. **11**(2), 10–14 (2013).
24. M.N.A. Rahman, A.F.A. Abidin, M.K. Yusof, N.S.M. Usop, Cryptography: a new approach of classical Hill cipher. Int. J. Secur. Its Appl. **7**(2), 179–190 (2013).
25. D.C. Mishra, R.K. Sharma, R. Ranjan, M. Hanmandlu, Security of RGB image data by affine hill cipher over SLn(Fq) and Mn(Fq) domains with Arnold transform. Optik **126**, 3812–3822 (2015).
26. B. Acharya, M.D. Sharma, S. Tiwari, V.K. Minz, Privacy protection of biometric traits using modified Hill cipher with Involutory key and robust cryptosystem. Procedia Comput. Sci. **2**, 242–247 (2010).
27. K.A. Reddy, B. Vishnuvardhan, Madhuviswanatham, A.V.N. Krishna, A modified Hill cipher based on circulant matrices. Procedia Technol **4**, 114–118 (2012).
28. N. Sharma, S. Chirgaiya, A novel approach to Hill cipher. Int. J. Comput. Appl. **108**(11), 34–37 (2014).