Securing electronic health system using crystographic technique

Yunusa Simpa Abdulsalam*,
Olayemi Mikail Olaniyi and Aliyu Ahmed

Computer Engineering Department,
Federal University of Technology Minna,
Niger State, Nigeria
Email: abdulsalam.pg611937@st.futminna.edu.ng
Email: mikail.olaniyi@futminna.edu.ng
Email: aliyu.ahmed@futminna.edu.ng
*Corresponding author

Abstract: Telemedicine application mostly takes place in advance settlements, where important medical information is to be effectively secured and transmitted on public networks. Whilst the data is accessed by an illegitimate individual, it may lead to malicious attack or any modification of medical image can result in misdiagnosis. The notion of medical information storage in automated form arose immediate concerns about healthcare data security and privacy. The need to design a secure distributed system to provide adequate authentication of patient data and confidentiality of patient medical record becomes imminent. This paper addresses confidentiality issues of electronic health record (EHR) in clinic tele-diagnostic system using crystographic technique. The developed crystographic algorithm embraces discrete wavelet transform (DWT) steganography technique instead of the traditional least significant bit (LSB) technique thereby providing required data robustness, payload capacity and imperceptibility of patient data over tele-consultation in Tele-clinic diagnostic scenario. Results of quantitative performance evaluation of host medical image of the EHR system showed an encrypted imperceptible and robust stego image of peak signal to noise ratio (PSNR) greater than 40 db. Results of evaluation portray a system capable of providing countermeasures against eavesdropping attack in data communication networks in clinic tele-consultations.

Keywords: confidentiality, electronic health record; EHR; authentication; security; tiny encryption algorithm; TEA.

Reference to this paper should be made as follows: Abdulsalam, Y.S., Olaniyi, O.M. and Ahmed, A. (2019) 'Securing electronic health system using crystographic technique', *Int. J. Telemedicine and Clinical Practices*, Vol. 3, No. 2, pp.132–155.

Biographical notes: Yunusa Simpa Abdulsalam obtained his BEng in Electrical/Computer Engineering and Masters of Computer Engineering in 2015 and 2017, respectively, from Federal University of Technology, Minna, Nigeria. He is currently a PhD candidate in Data Science, Networking and Algorithm Thinking (DNA) at University Mohammed VI Polytechnic. He is a promising computer network security expert. His research interests are in distributed systems design, wireless sensor networks, privacy and computer network security.

Olayemi Mikail Olaniyi is a Senior Lecturer in the Department of Computer Engineering at the Federal University of Technology, Minna, Niger State, Nigeria. He obtained his BTech and MSc in Computer Engineering and Electronic and Computer Engineering respectively. He had his PhD in Computer Security from the Ladoke Akintola University of Technology, Ogbomosho, Oyo State, Nigeria. He published in reputable journals and learned conferences. His areas of research include information and computer security, intelligent/embedded systems design and telemedicine.

Aliyu Ahmed is a Lecturer II in the Department of Computer Engineering at the Federal University of Technology, Minna, Niger State, Nigeria. He obtained his BEng in Electrical and Electronic Engineering from the Federal University of Technology Minna and his MSc in Computer Networking from the University of Bedfordshire, UK. He is currently a doctoral student at the Department of Computer Engineering Federal University of Technology, Minna, Niger State, Nigeria. His research interest include computer security, intelligent systems, embedded systems and wireless sensor networks.

1 Introduction

The recent trends in information technology have progressively transformed populace standard of living (Vallathan et al., 2016). The Internet confers an expedient atmosphere for users to interchange covert data with others irrespective of their residence. Telemedicine is one such application provided by internet for the prompt delivery of healthcare info across distanced locations. It entails information transfer about health-related matters between individuals and health canters. Telemedicine has played a significant role by using the internet and other relevant technologies in providing services to distance patients far from doctor's location, and as well reducing transportation cost (Acharya et al., 2011). Telemedicine has demonstrated a lot of benefits, ranging from modified access to personal medical information, cost effectiveness in treatment and an effective care delivery (Ben-Assuli, 2015). Though with this salutary benefits, it has also portrayed limitations such as maintaining high security of patient transmitted data and quality of received medical image (Anderson and Agarwal, 2011). It is vital to securely transmit and preserve patient's data along with its respective medical image.

Transferring secured medical images in electronic health records (EHR) has become a salient issue in networked environment (Santhi and Adithya, 2017; Abdulsalam et al., 2018). The dependability and consistency in providing effective medical access without unofficial alterations is the basic function of every health service provider. As more vital data is stored in EHR systems, the need for appropriate security for authorised access to EHRs becomes gradually critical. Analysis carried out by Health Information Trust (HITRUST) Alliance for US medical data break-ins (Hourihan and Cline, 2012) reported most breaches to healthcare was as a result of theft. In 2009, after issuing a breach notification rule, a total number of 538 break-ins affecting over 21.4 million patient record was reported (Redspin, 2011). Also a report by Symantec (2013), showed that a total number of 146 break-ins affecting close to 3 million individuals was reported. IBM (2018) data breach reports that there has been a 10% decrease in data breach report that cost US$3.62 million dollars. Despite the high general decline decrease, companies and health patient's information are found to have the highest data breaches. This has been a very high demanding factor in the dark-market, where a single stolen health medical data is being sold for over US$363, making it the most expensive worth of information compared to any other stolen information (IBM, 2018). In Africa, healthcare financing is as a result of budgetary allocations, out-of-pocket expenditure, development finances from non-governmental organisations (NGOs) and a considerable contribution from social health insurance donations. In Nigeria, close to 80% of total health expenses is recorded as out-of-pocket expenditures, placing a financial drain on the poor. Currently, the Nigeria National Health Insurance Scheme (NHIS) is limited to mostly employed individuals and the formal public sector. In 2016 National Living Standard Survey, 22,000 households were sampled: out-of-pocket expenses on medical care was reported to be roughly US$33.5 per capita, this accounted for nearly 19% of entire household expenses. Further survey by NHIS (2017) reported 54% out of pocket spending and 10% of the total population who self-medicate due to lack of proper guarantee schemes set in place. The remaining 36% are enrolled in health insurance scheme, where 96% are employed and earn more than US$ 285.

Nevertheless, it would not be pointless to also mention that the services provided by telemedicine increases access to healthcare and improves healthcare outcomes. Despite all these highlighted advantages, telemedicine has severe security and privacy issues such as confidentiality, integrity, authentication and availability, which needs to be addressed especially when it is related to patient information. The need to create a secure channel of communication between patients and practitioners is deemed necessary. Therefore, security restrictions such as user authentication, data confidentiality and medical image integrity are to be effectively managed.

It is of no doubt that information hiding has posed the greatest challenge and deciding factor on usage in modern technological world. Different methodologies have been adopted in the past to secure medical data in transmission channels. This ranges from steganography, cryptography and watermarking. In recent times, the collective adoption of cryptography and steganography to design a novel robust technique has been an effective means of information hiding. These techniques are segregated into sub-categories as encryption, steganography and crystography or simultaneous combination of cryptography and steganography (Olaniyi et al., 2017). In steganography, security is achieved by embedding the secrete message in an image. The resulting image is called a stego image. Medical information represented in digital form offers several advantages, such as wide distribution of multiple flawless duplications of the original content (Kaur and Kaur, 2016). In numerous conditions, alternations to content aid legitimate purposes. Though, in other circumstances, the alterations may be intentional and can accidentally have effect on the content interpretation.

This paper addresses confidentiality issues surrounding EHR system in clinic tele-diagnosis using crystographic technique. Crystography emphasises the synergistic mixture of data hiding schemes of cryptography and steganography for proper enhancement of security communications over public network (Gabriel et al., 2013; Olaniyi et al., 2015). Crystography in the context of this work, involves securing EHR data transactions using Huffman algorithm, LBG encryption algorithm and transform-based discrete wavelet steganographic algorithm as opposed to the works of Solichin and Ramadhan (2017) and Saxena et al. (2018).

The quantitative performance evaluation of the developed crystographic technique was carried out using MATLAB® image processing toolbox based on three performance evaluation metrics; PSNR, mean squared error (MSE) and image histogram.

The remainder of this paper is organised into five sections, Section 2 presents review of related works, system methodology is provided in Section 3, while discussion of results is presented in Section 4. Conclusion and scope for future works is presented in Section 5.

2 Review of related works

A basic necessity in securing patient information is to properly authenticate patient electronic record, specifically the stored images. More regularly, a header or attached files, which conveys all the required data, by correctly identifying the stored image. Nevertheless, storing the meta-data of an image into separate headers or files is liable to clumsy practices. An option is to embed or implant such information in the image itself. The research that are precisely focused on medical image watermarking are few. While some of the techniques adopted in the past may seem to have minimal effect on the diagnostic content, for instance, the least significant bits (LSB) plane manipulation is well known, as a result of the fact that it less robust and perceptibility is very poor.

In the early years of steganography, Macq and Dewey (1999) presented a trusted header technique by inserting the file header hashing of medical image in raw files, Miaou et al. (2000) then proposed a crystographic LSB plane insertion. In this technique, the host or original image validates the embedded message composing of several patient information, such as doctors signature and diagnosis medical report. Coatrieux et al. (2001) proposed a region of interest (ROI) to safeguard the region of non-interest (RONI) which served as the watermark carrier. An image virtual border as area for watermarking was proposed by Trichili et al. (2002). In this method, medical data was embedded in the LSBs plane. Cao et al. (2003) proposed a technique where the whole image digital stamp is embedded. Cao et al. (2003) further extended the research on digital envelope (DE) by embedding the DE in an unpredictable sequence and replacing the LSB insertion of every chosen pixel. All these studies mentioned focused on embedding the medical images in either ROI or RONI, as these were the troubling issues of the time, but as research evolves, an issues of compression and encryption of medical images arise.

A reversible watermarking scheme was proposed by Guo (2008), the scheme was aimed at protecting EHRs by the use of biometric patient recognition system. The main objective of the technique was to implement a scheme that will best store delicate data, at the same time protecting patient's privacy. The methodology adopted was integer wavelength transform (IWT), which successfully created an insertion space in the high frequency sub-bands. Part of the limitations to the work was that it lacks simplicity and prone to image attacking manoeuvres such as filtering, compression, and additive noise.

Brifcani and Brifcani (2010) proposed a similar crystographic technique which implemented stego-based-crypto scheme by simultaneous combining lifting wavelet transform stenographic algorithm and RSA cryptographic algorithm. The adopted cryptographic algorithm was utilised to further enhance the developed system's security. The scheme utilised two different approaches for data embedding; firstly, embedding in the low frequency sub-band and secondly, embedding in all sub-bands. Both these methods attained high imperceptibility enhancement. Part of the strength to the work was high image precision but a limitation to the unacceptable number of characters that can be embedded.

Subsequently, Olaniyi et al. (2015) implemented advanced encryption standard (AES) cryptographic scheme in securing patient data confidentiality, the technique utilised a web real-time communication (WRTC) for clinical tele-consultation. The performance evaluation of the developed system depicted that it could further enhance healthcare in developing countries. The system proved to have increased security, enhanced productivity and better efficiency of health delivery. However, the system security can be further enhanced for automatic identification and data confidentiality.

Steganography is majorly implemented in two ways, frequency or spatial domain. The frequency domain implementation is known as image transform coefficient. Many of the prevailing transform coefficient techniques are mostly implemented in frequency domain, which can be either in discrete wavelet transform (DWT), discrete cosine transform (DCT) or contourlet transform (CT). From literature, steganography implemented in the spatial domain proves to be weak and its content could easily be altered whenever the resulting cover image is being corrupted (Kumar and Kalpana, 2015). Spatial domain methods like LSB substitution, spread spectrum, etc. are trouble-free, support huge amount of data embedding in the medical image but not robust (Vallathan, et al., 2016). The most significant portion in a medical image is known as ROI. This portion becomes less robust when data embedding is done in spatial domain. However, different transform spheres (DFT, DWT, and DCT) are additionally robust to the same signal processing attack. This fact necessitates that the operations must be made in transform domain, to maintain the above requirement.

In this paper, a digital message hiding scheme is proposed for the combination of steganography and cryptography, crypt-steganography or crystography using LBG algorithm and Huffman compression algorithm. The combination of these two techniques satisfies the requirements such as high security and robustness between sender and receiver. The technique guarantees suitable high medical image quality with very little alteration in the resulting image. The main benefit of the entire approach includes the fact that the LBG algorithm is very secure and the DWT transformation technique is very hard to detect in image steganography. It also produces efficient robustness of stego-image. The major aim is to develop a security system that data embedded in an image (secrete message) cannot be easily retrieved by any attacker in the communication process.

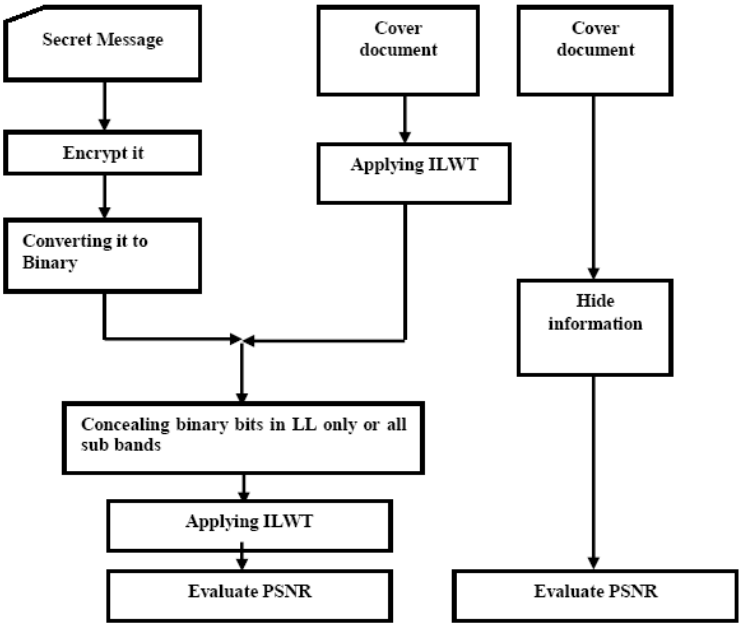
3 Methodology

Information hiding in images has stern restraints such as high robustness, imperceptibility and capacity (Singh and Chadha, 2013). Simultaneously realising these requirements can most times prove to be very cumbersome. These restrains can be accomplished by means of appropriate data hiding technique, such as steganography and watermarking technique, which are suitable for proper implementation of telemedicine applications. EHRs and information hiding for telemedicine applications demand medical data to be effectively concealed and easily revocable in other to maintain information integrity, availability and the confidentiality medical data. Digital image watermarking techniques can be categorised in three classes: authentication technique; data-hiding technique; and schemes that combines data hiding and authentication (Kaur and Kaur, 2016). Authentication and validation schemes can be used to categorise the real source of the original image, and tamper recognition can be used also to detect the areas where tampering was done. In most circumstances, tampered regions are mostly recovered. Information hiding techniques offers more significance in embedding large volume of information in images and as well try to maintain high imperceptibility. Subject to the condition of these three watermarking categories to be adopted, a suitable steganography or watermarking technique is then chosen accordingly.

3.1 Steganography technique in information hiding

Steganography has been vastly utilised in several areas of application to preserve the confidentiality and integrity of messages transmitted using internet (Guha and Sarmah, 2015). The need to conceal information has tremendously increased as a result of high fraudulent and malicious activities in cyber space. Steganography by definitions refers to the art and science of concealing undisclosed information in another media (Shikha and Dutt, 2014). The data to be concealed is known as the secrete message and the medium by which data is concealed is known as cover image or document. The document encompassing the secret or concealed message is known as the stego image or document. The stego-system is the process implemented when concealing the information in the medium at the transmitting end and extracting the concealed information at the receiver's end.

Figure 1 Steganography technique



Source: Brifcani and Brifcani (2010)

Steganography is a data concealing technique, employed to hide data in another medium known as the cover image or document by altering its original properties, as represented in Figure 1. There exist different approaches when categorising steganography systems. It could be classified according to the type of cover used for communication.

3.2 The developed wavelet image crystographic algorithm

The objective of image compression as applied to the developed algorithm is to minimise image redundancy and to transmit or store patient's information in an efficient and efficient form. The goal of which such is to minimise storage quantity as efficiently as possible. Lossless compression is a compression algorithm in which the original image can be completely recovered from the compressed image without any loss. Some of the popular lossless compression techniques are run length coding, Huffman coding, arithmetic encoding, entropy and area coding.

Run length coding is a simple method used for compressing sequential data. It achieves compression by reducing redundancy and avoiding repetitive data. The mixture of a run-length coding scheme simultaneously followed by Huffman coder formulates the standard image compression basis. These image compression standards are said to yield decent compression ratios from 20:1 to 50:1 (Rani and Lakshmanan, 2016). In the developed crystographic scheme, run length encoding was used to compress the image followed by a Huffman coder. The special feature of this algorithm is data hiding combined with appropriate compression algorithm.

To provide complete security to the system, encrypted data was concealed in an image as a whole. Before the transmission process, the data concealed image is encrypted using LBG algorithm. Initially the image is converted into sequence of blocks called vectors, representing the entire image. Consider the original image X and the vectors $\{X_1, X_2, X_3, \ldots\ldots, X_m\}$, where m represents the number of code vectors. For each and every vector code, vectors are represented in the code book. So, Y be the codebook containing $\{Y_1, Y_2, Y_3, \ldots\ldots, Y_n\}$, where n is size of the codebook. For encoding the image vector X' a suitable Y' is selected such that there exists a minimum distance between them. This is the Euclidean distance and expressed as

$$d\left(X_i Y_j\right) = \left\|X_i - Y_j\right\|^2 = \sum\left(X_{i1} - Y_{j1}\right)^2 \tag{1}$$

where i and j 1, 2, 3, ……, u.

Here X_{i1} and Y_{j1} represent the 1th element of X_{i1} and Y_{j1} respectively.

Using an index j of Y_j is used to replace X_i.

Similarly, in decryption process, the code words are collected for decryption. This algorithm also compresses the image before encryption process to achieve a better compression ratio. Pseudo random numbers are generated during the time of encryption which is significant to decrypt the stego document along the receiver end. Figure 2 represents the flow chat for the embedding and extraction algorithm as represented below.

3.2.1 Embedding procedure

```
      Begin
Input:
      An $M \times N$ carrier image and a secret message/image.
Output:
      A stego-image.
1     Acquire Huffman table of secret message.
2     Obtain Huffman encoded bit stream of secret-image by utilising the Huffman table of
      secrete acquired in step 1.
3     Use Haar wavelet transform to decompose the cover document.
4     Compute the size of the bit stream.
5     Iterate for each bit acquired in step 4.
6     Place 3 successive bits into the position of every wavelet transform coefficient of the
      chosen LL band.
7     For every bit acquired in step 2. place 3 successive bits into 3 locations in every wavelet
      transform coefficient of the chosen band.
8     For every bit in the Huffman table. Place 3 successive bits into 3 LSB locations of every
      wavelet transform coefficient of the chosen sub-band.
9     Apply the inverse of DWT.
10    End.
```

Algorithm 1 Embedding algorithm

```
Begin
   Input:
   An $M \times N$ carrier image and a secret message/image.
   Output:
   A stego-image.

   Obtain Huffman table of secrets
   for columns = 1:8:
   1,024 previous Dwt =
   0;
   for rows = 1:8:1024
   first Dwt = previousDwt – subZigzagArray(1);
   Runlength
   coding
   count = 0;
   p = 2;
   runLenCoding = 0;

   LBG algorithm coding
```

```
    Image [M, N] = size(x);
    [M2, P] = size(y);
    Matrix dimensions do not match if (M ~= M2),
    Euclidian distance d = zeros (N,P);
    d (n, :) = sum((x(:, n + copies) – y) .^2,1), if (N < P)
    d(:, p) = sum((x – y(:, p + copies)) .^2,1), for p = 1:P, end

    txt = [txt,’\’];

    img(i, j) = new_pixel;
    end
    end
```

3.2.2 Extraction procedure

```
    Begin
Input:
    An $M \times N$ Stego-image.
Output:
    Secret image.
1   Apply DWT to stego document.
2   The extent of the coded bit stream is removed from the first four wavelet transform
    coefficients in every sub-band.
3   3 least bits of the DWT coefficient are collected.
4   Continue step 3 until the size becomes equal to the one extracted in step 2.
5   Construct Huffman table of secrete by removing 3 bits of all wavelet transform coefficients
    in every sub-bands.
6   Decrypt the selection gotten in step 3 by using Huffman table.
7   End.
```

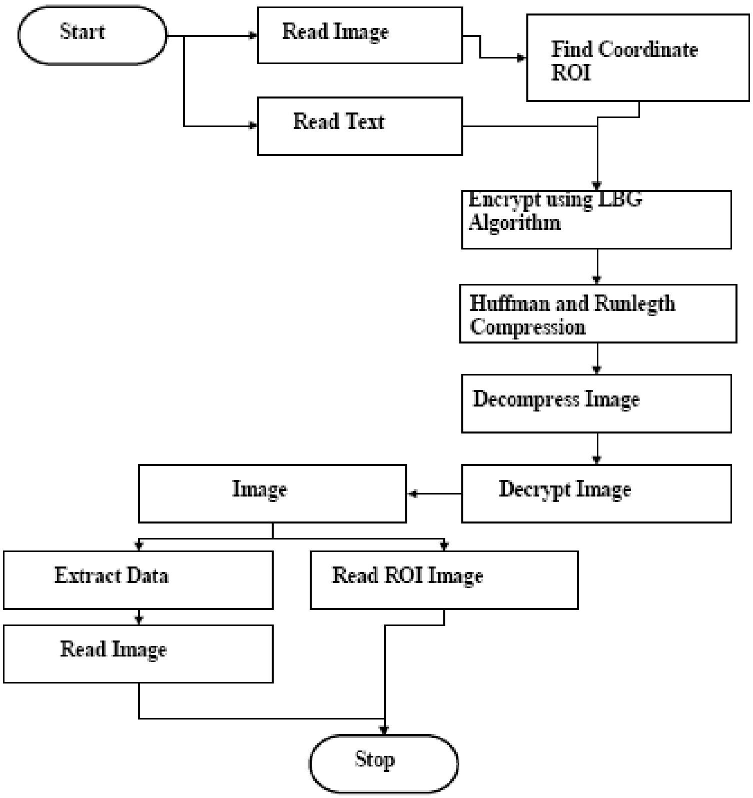
Algorithm 2 Decryption algorithm

```
Begin
    Input:
    An $M \times N$ stego-image.
    Output:
    Secret image.

    [l, m] = size(img);
    temp_pixel= img(i,j);

    Construct Huffman table of secrete by removing 3 bits of all wavelet transform coefficients
    in every sub-bands.
```

Decrypt the selection

End.

Figure 2 Flow chart of embedding and extraction algorithm



3.3 System experimental and performance evaluation procedures

There are several metrics used in this work to evaluate the image steganography technique used on the EHR system. They are: MSE and PSNR metrics computations, image histogram visualisations and human visual perpetuations. MSE denotes the collective squared error in original and output image. The lesser the significance of the squared error, the lesser the error and this can be calculated using equation (2).

$$MSE = \frac{1}{4MN} \sum_{i=1}^{2M} \sum_{j=1}^{2N} \left(C_{ij} - S_{ij}\right)^2 \tag{2}$$

where C_{ij} represents the value of the original image pixel, S_{ij} represents the value of the output image pixel, M and N are represented as rows and columns respectively in the original image.

The peak signal to noise ratio (PSNR) block computes the PSNR value, represented in decibels, between the two images. The ratio obtained is mostly used as quality measurement between original and stego image. The more the PSNR value, the better the quality of the stego image. This can be calculated using equation (3).

$$PSNR = 10\log_{10}\frac{\left((2^b-1)^2\right)}{MSE}dB \tag{3}$$

These two performance metrics are inversely proportional to each other. The value of PSNR increases when two images are close to each other whereas the value of MSE decreases when the two images are similar to each other.

4 Results and discussion

4.1 Performance evaluation of the developed crystographic algorithm

The developed wavelets crystographic scheme in Subsection 3.2 was quantitatively evaluated using metrics such as PSNR, MSE and SSIM. Further qualitative evaluation was done using human visual system (HVS) with image histogram. Different metrics exist in literature for image analysis and the necessary ones has been adopted for evaluation of the original and stego images. Firstly, the quality of the stego images was checked with PSNR value. Generally, PSNR values below 30db signifies a fairly low image quality. While, the value of MSE decreases when the two images are similar to each other. A better quality stego image would strive for 40db above.

In the metrics result presented in Table 1, all PSNR value are greater than 70db. Which depicts very high quality as compared to HVS results in Tables 2, 3, and 4. The HVS comparison between cover image and distorted image after extraction for different host images, shows nearly no difference when looking with the human eye. The MSE as also computed in Table 1 shows the cumulative MSE between different cover images and stego image, as the rate of embedding is been increased (number of characters embedded). The algorithm presents stego image of which MSE calculated value are observed to have negligible differences that lies between 0.000007 to 0.00021. The structural similarity index (SSIM) as also shown in Table 1, which proves that the image similarity index is highly negligible and at an acceptable level. Figures 4–12 shows the histogram realisation of the original and stego images in red, blue and green channels, after concealing medical information respectively. For instance, Figure 4 shows the histograms of original image in Table 2. Histogram realisation in Figure 4 when compared to Figures 5, 6 and 7, indicates that the change in original and stego images is very low. Also, depicting high imperceptibility, Table 1 shows the rest of experimental MATLAB realisation results for PSNR, MSE and SSIM.

Figure 3 depicts the rate of embedding characters into different host images. Its observed that, as the rate of embedding increases, the PSNR reduces. In other words, affects the quality of the stego image.

Table 1 Metrics calculation of the realised images

Size	*Number of characters embedded*	*Chest*	*PSNR*	*MSE*	*SSIM*
512 * 512	250	Stego image 1	89.7237	0.00007	0.99999998
512 * 512	500	Stego image 2	87.5849	0.00011	0.99999997
512 * 512	750	Stego image 3	86.1582	0.00016	0.99999996
512 * 512	1,000	Stego image 4	85.1202	0.00020	0.99999995
		Brain			
512 * 512	250	Stego image 1	87.0102	0.00013	0.999999999
512 * 512	500	Stego image 2	84.0077	0.00026	0.999999997
512 * 512	750	Stego image 3	82.2493	0.00039	0.999999996
512 * 512	1,500	Stego image 4	81.0013	0.00052	0.999999995
		Fingers			
512 * 512	250	Stego image 1	90.7645	0.00055	0.999999998
512 * 512	500	Stego image 2	87.0178	0.00013	0.999999997
512 * 512	750	Stego image 3	85.5879	0.00018	0.999999996
512 * 512	1,000	Stego image 4	84.9099	0.00021	0.999999995

Figure 3 Number of characters against the quality of the image (see online version for colours)

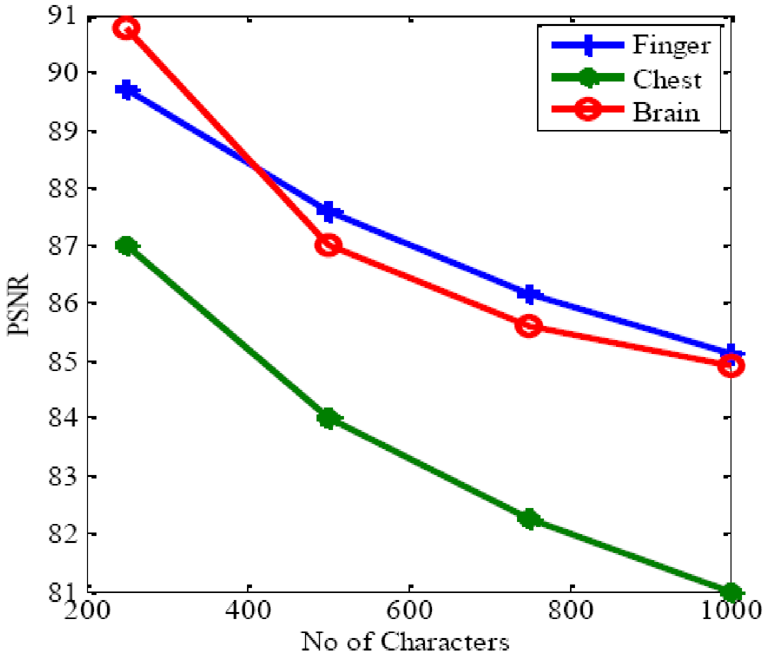


Table 2 HVS comparison of original image (chest) with corresponding stego images

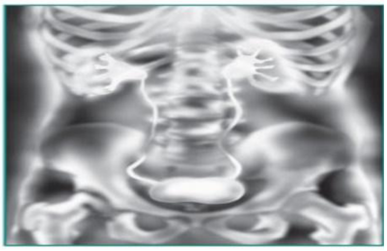
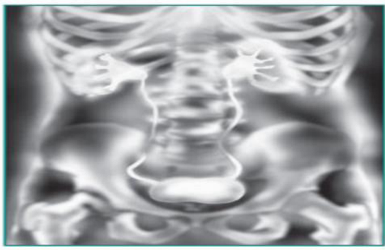
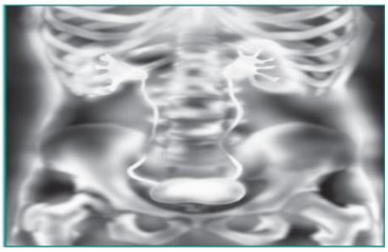
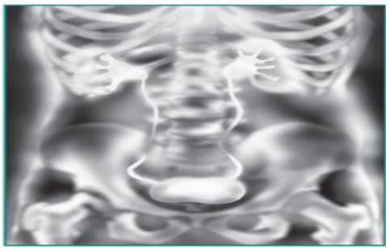
Original image (chest)	*Stego image 1 (250 characters embedded)*
	
Stego image 2 (500 characters embedded)	*Stego image 3 (750 characters embedded)*
	

Table 3 HVS comparison of original image (brain) with corresponding stego images (see online version for colours)

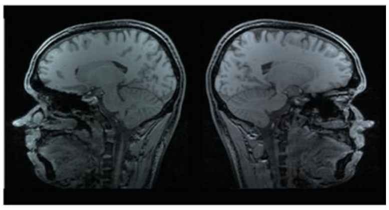
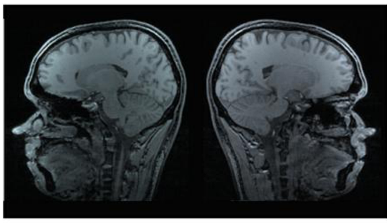
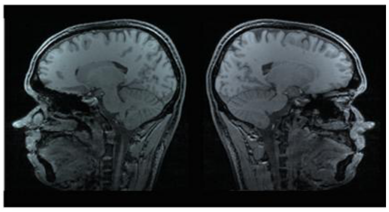
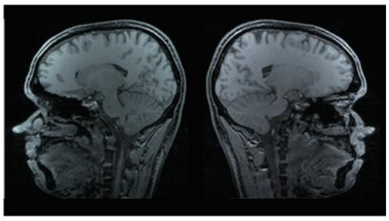
Original image (brain)	*Stego image 1 (250 characters embedded)*
 ●	 ●
Stego image 2 (500 characters embedded)	*Stego image 3 (750 characters embedded)*
 ●	 ●

Table 4 HVS comparison of original image (finger) with corresponding stego images

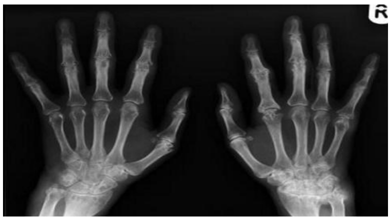
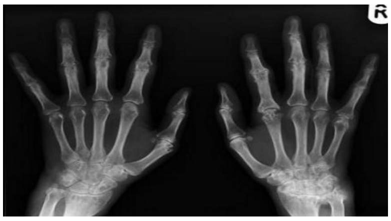
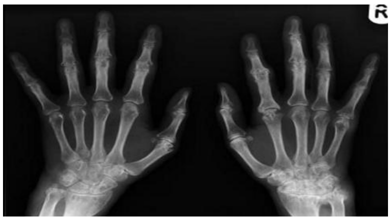
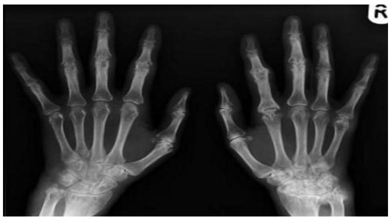
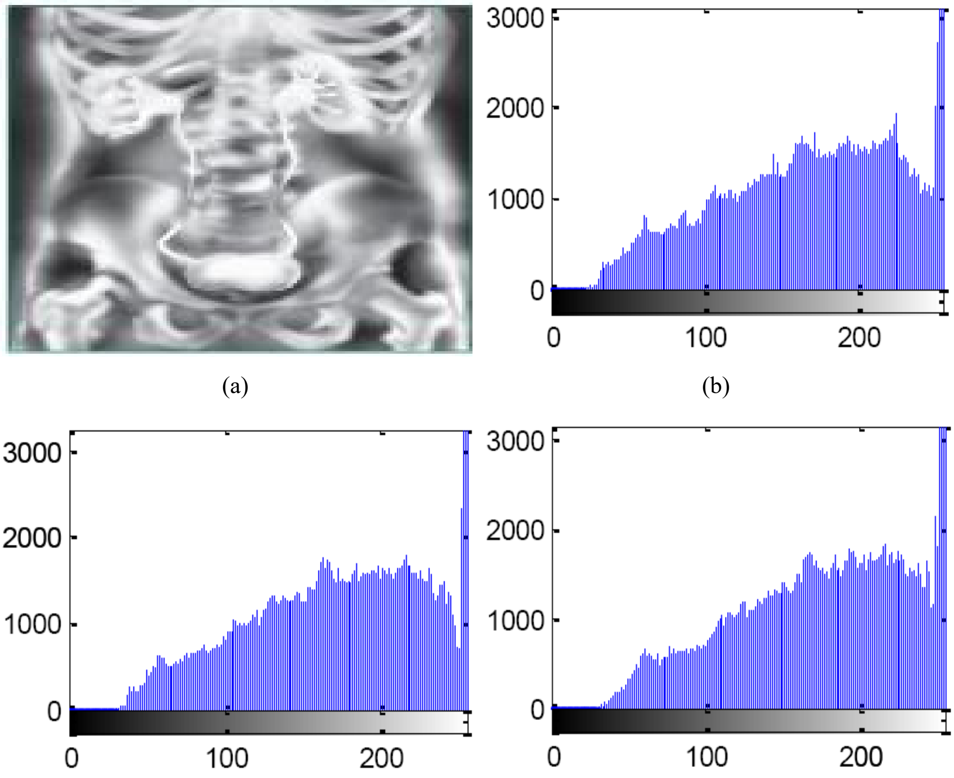
Original image (fingers)	*Stego image 1 (250 characters embedded)*
	
Stego image 2 (500 characters embedded)	*Stego image 3 (750 characters embedded)*
	

Figure 4 Histogram realisation of original image (chest), (a) original image (b) red (c) green (d) blue (see online version for colours)



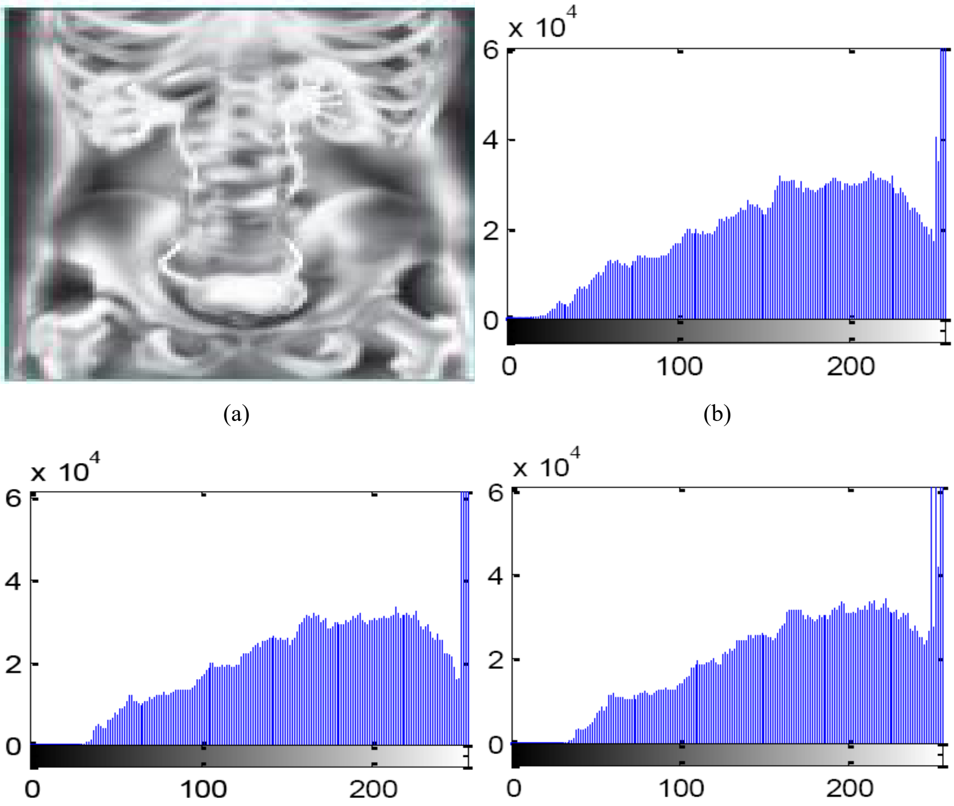
(a)

(b)

(c)

(d)

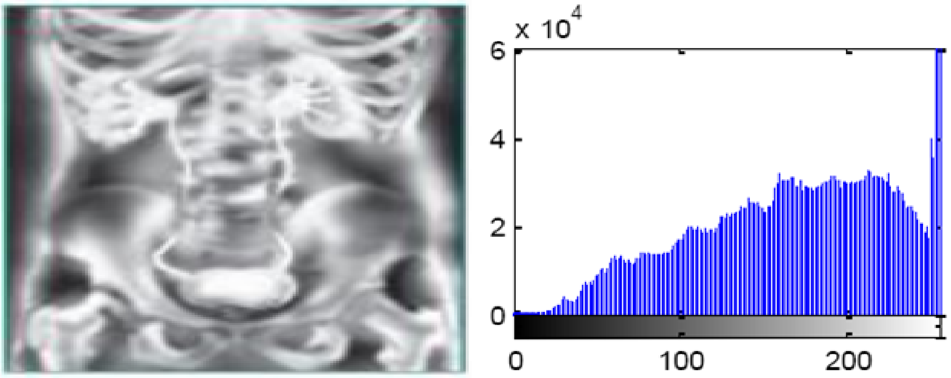
Figure 5 Histogram realisation of stego image 1 (chest), (a) stego image 1 (b) red (c) green (d) blue (see online version for colours)



(a) (b)

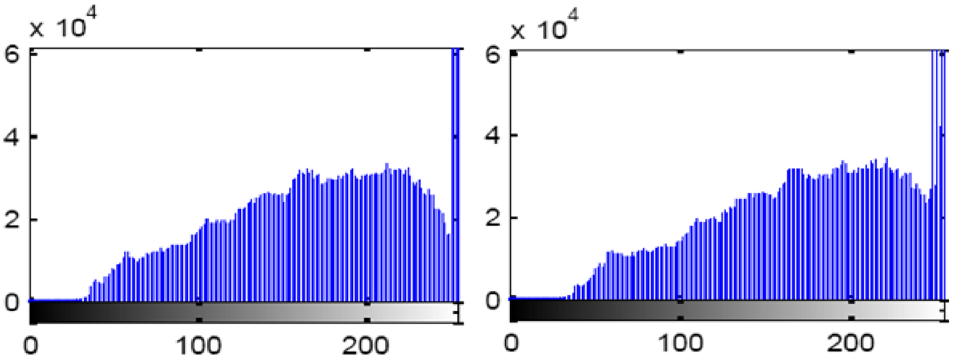
(c) (d)

Figure 6 Histogram realisation of stego image 2 (chest), (a) stego image 2 (b) red (c) green (d) blue (see online version for colours)



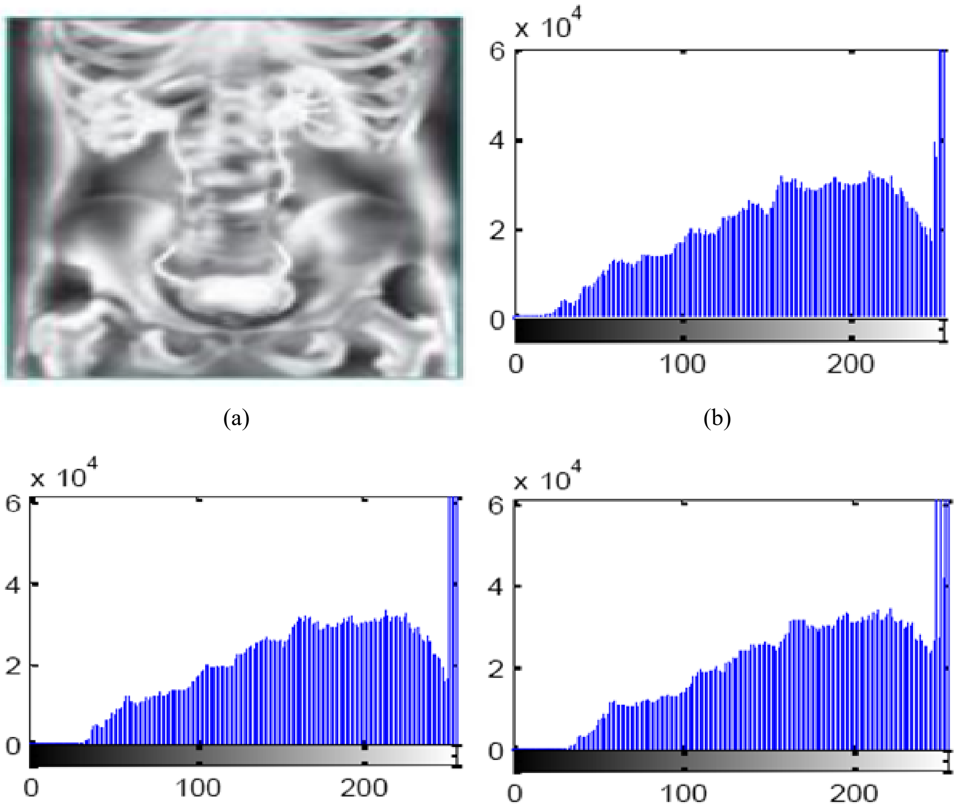
(a) (b)

Figure 6 Histogram realisation of stego image 2 (chest), (a) stego image 2 (b) red (c) green (d) blue (continued) (see online version for colours)



(c) (d)

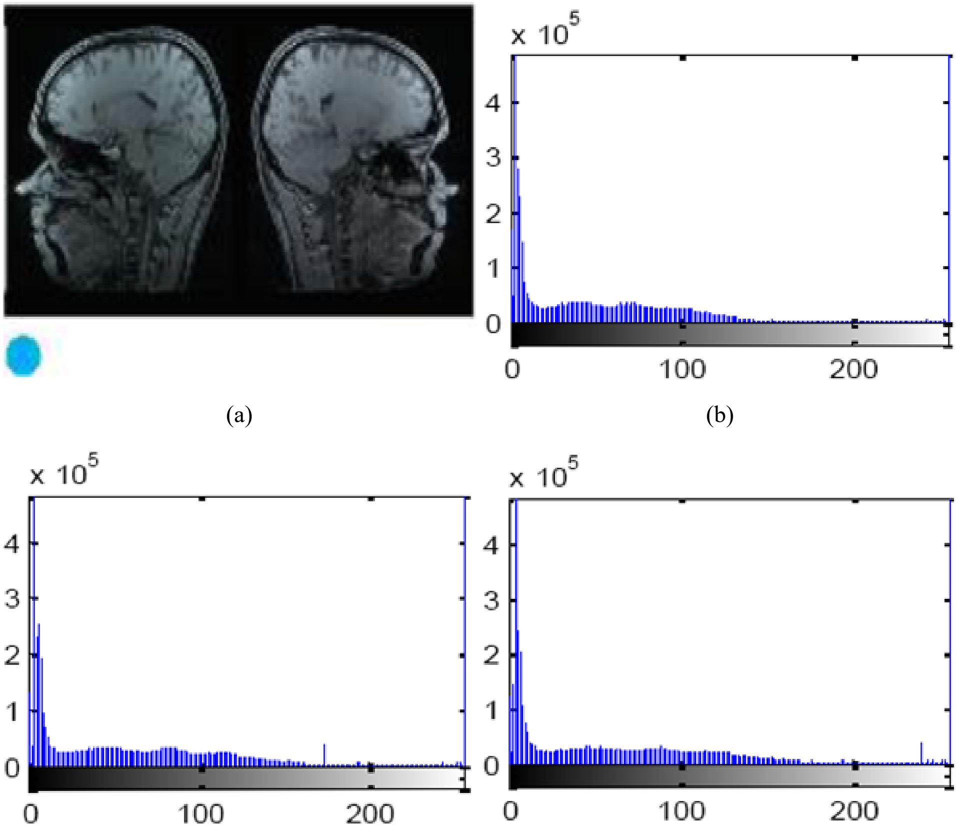
Figure 7 Histogram realisation of stego image 3 (chest), (a) stego image 3 (b) red (c) green (d) blue (see online version for colours)



(a) (b)

(c) (d)

Figure 8 Histogram realisation of original image (brain), (a) original image (b) red (c) green (d) blue (see online version for colours)



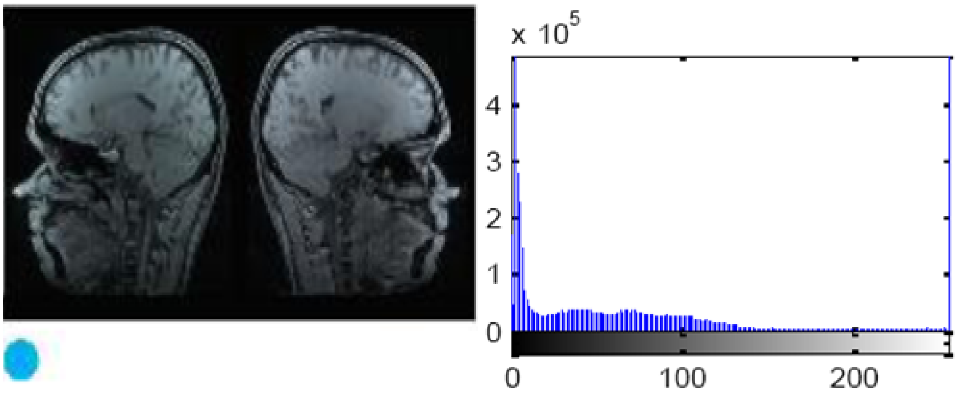
(a)

(b)

(a)

(d)

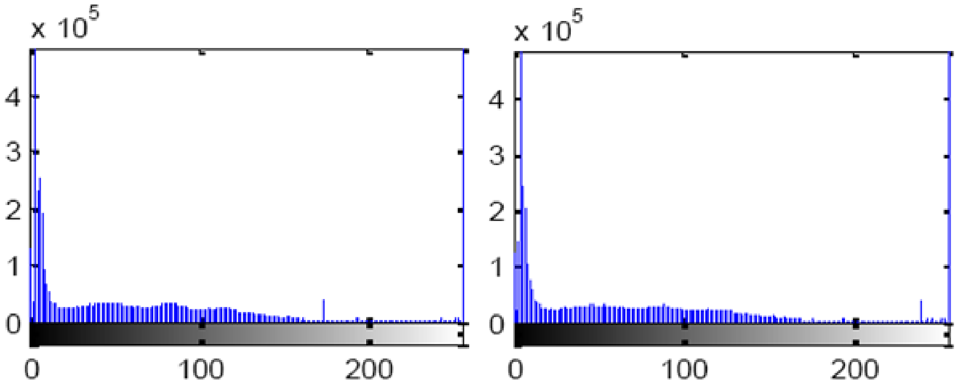
Figure 9 Histogram realisation of stego image 1 (brain), (a) stego image 1 (b) red (c) green (d) blue (see online version for colours)



(a)

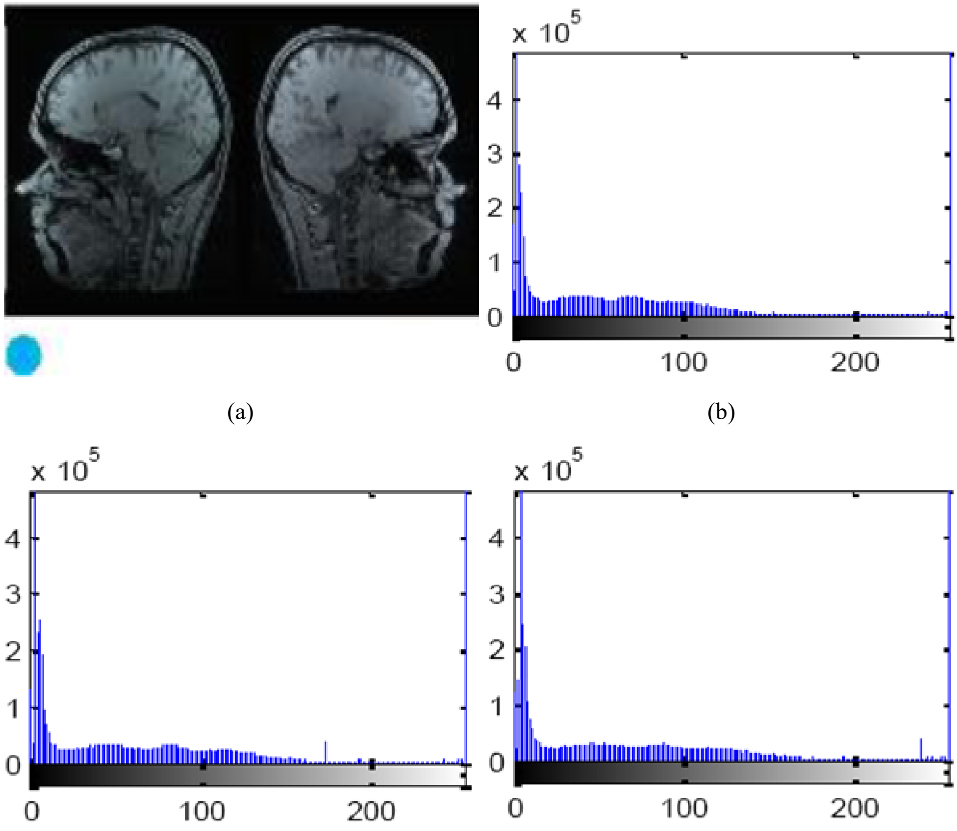
(b)

Figure 9 Histogram realisation of stego image 1 (brain), (a) stego image 1 (b) red (c) green (d) blue (continued) (see online version for colours)



(c) (d)

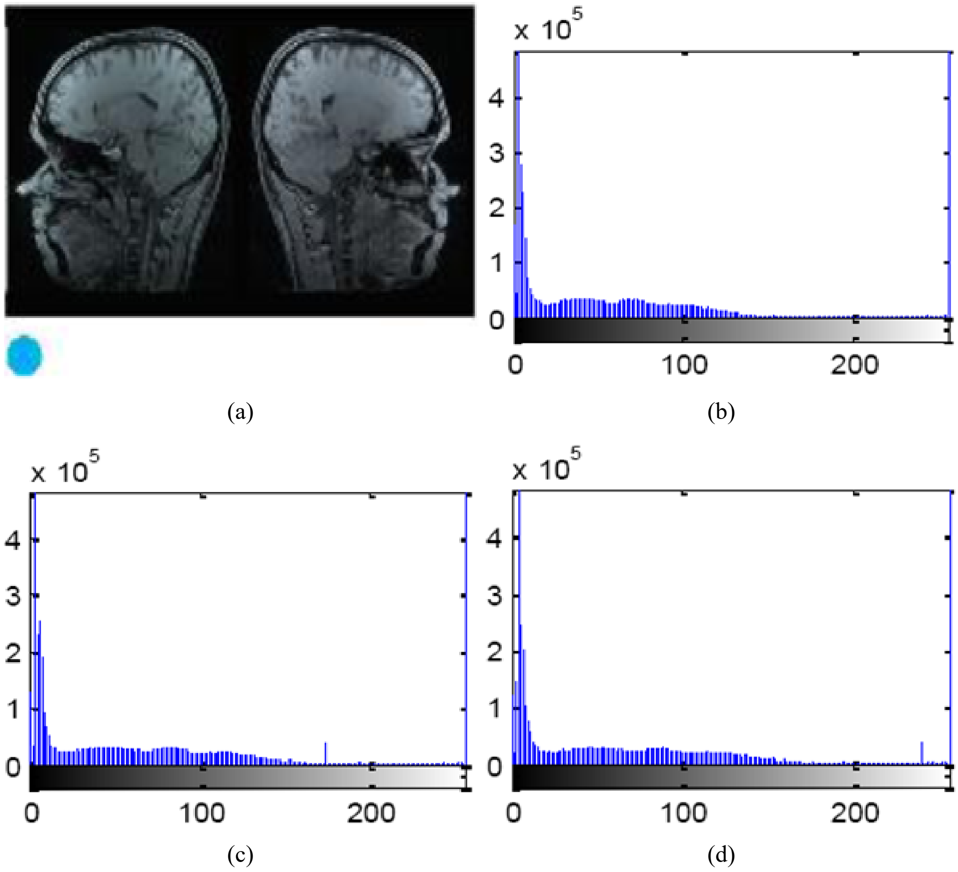
Figure 10 Histogram realisation of stego image 2 (brain), (a) stego image 2 (b) red (c) green (d) blue (see online version for colours)



(a) (b)

(c) (d)

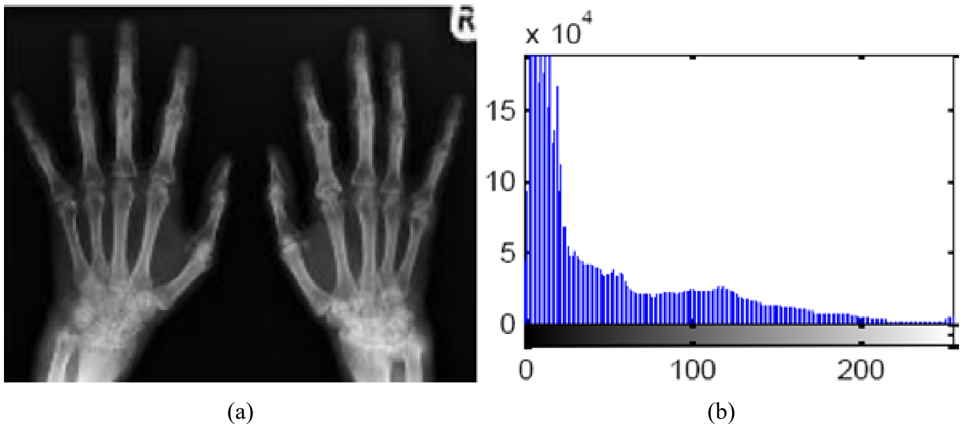
Figure 11 Histogram realisation of stego image 3 (brain), (a) stego image 3 (b) red (c) green (d) blue (see online version for colours)



(a) (b)

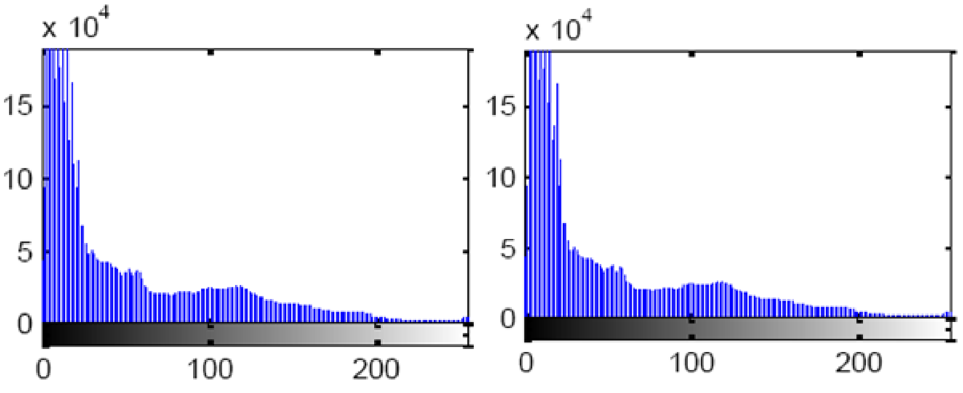
(c) (d)

Figure 12 Histogram realisation of original image (finger), (a) original image (b) red (c) green (d) blue (see online version for colours)



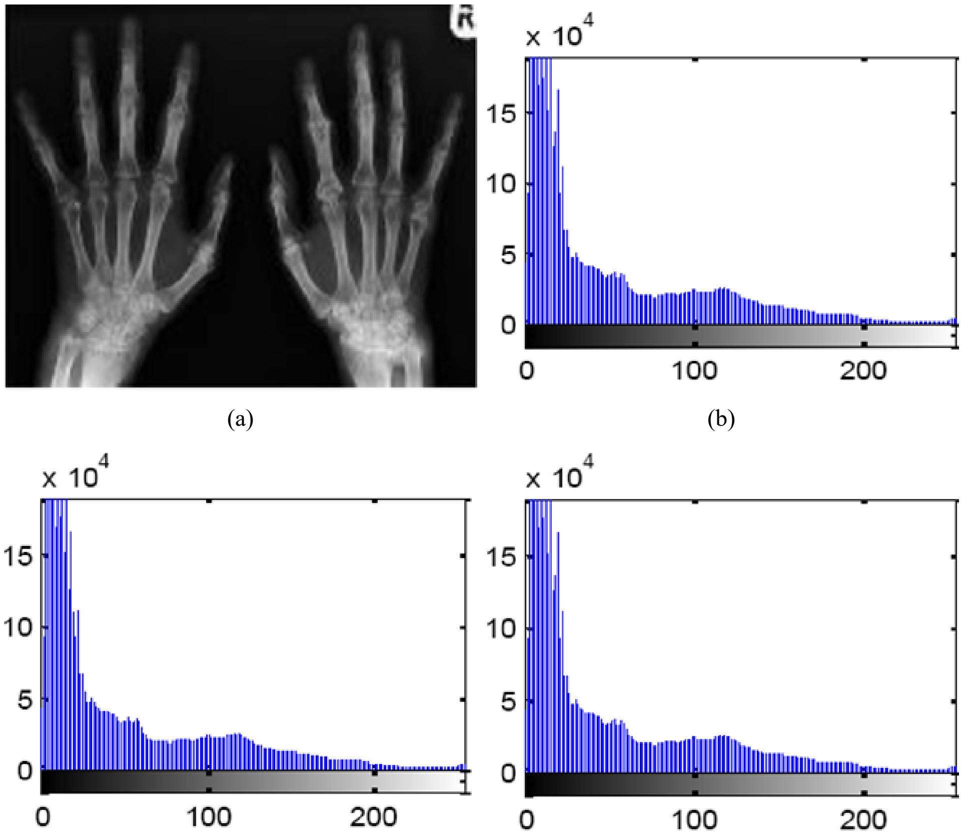
(a) (b)

Figure 12 Histogram realisation of original image (finger), (a) original image (b) red (c) green (d) blue (continued) (see online version for colours)



(c) (d)

Figure 13 Histogram realisation of stego image 1 (finger), (a) stego image 1 (b) red (c) green (d) blue (see online version for colours)



(a) (b)

(c) (d)

Figure 14 Histogram realisation of stego image 2 (finger), (a) stego image 2 (b) red (c) green (d) blue (see online version for colours)

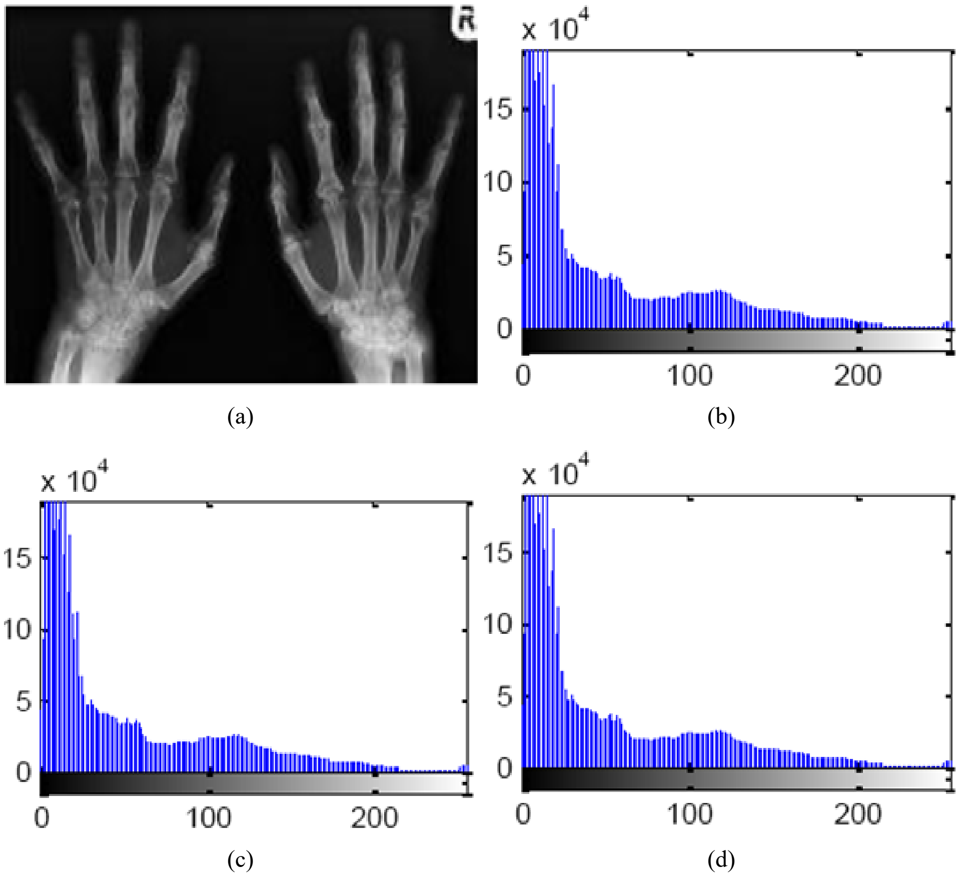


Figure 15 Histogram realisation of stego image 3 (finger), (a) stego image 3 (b) red (c) green (d) blue (see online version for colours)

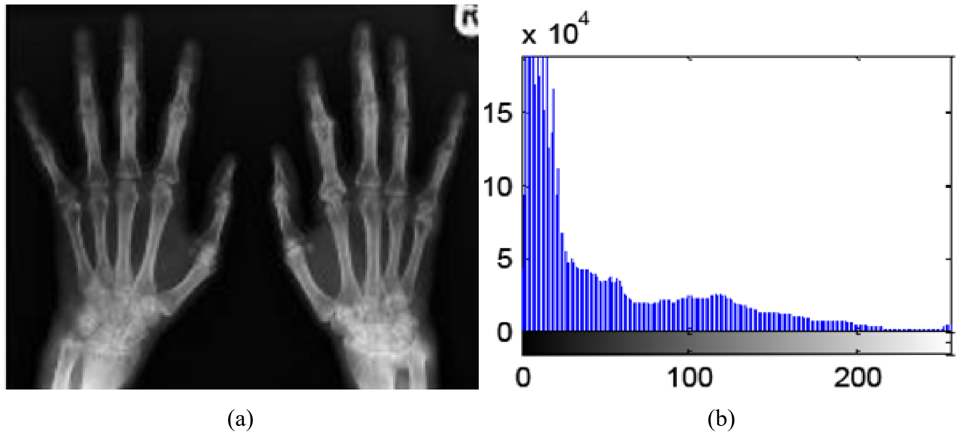
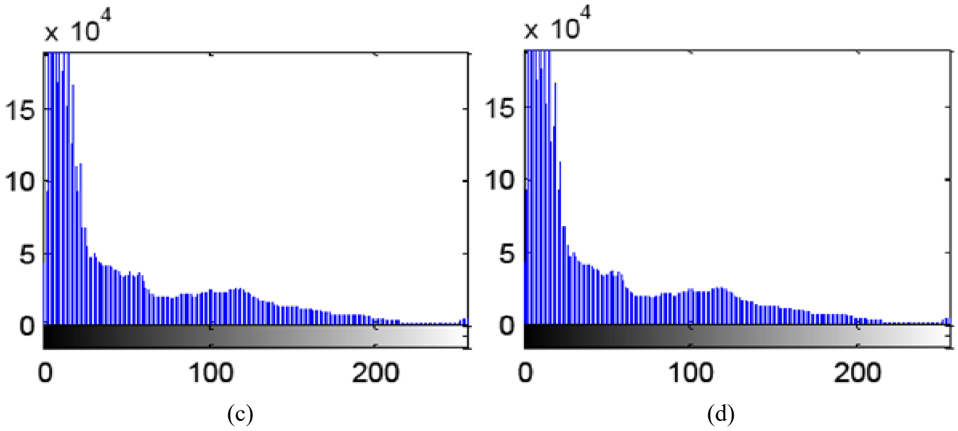


Figure 15 Histogram realisation of stego image 3 (finger), (a) stego image 3 (b) red (c) green (d) blue (continued) (see online version for colours)



(c) (d)

5 Conclusions and scope for future research

The development of an enhanced image crystography algorithm for patient medical confidentiality has been presented in this paper. The crystographic algorithm was effectively implemented to hide patient's information in therapeutic form, for example, CT, MRI, and X-ray scans. This technique bears secluded transmission alongside confidentiality in telemedicine applications. This change effectively symbolises multi-scale and multidirectional singularities of a picture and accomplishes superiority to the LSB with less artefacts, and enhances smoothness in the recreated images. The scrambling matrix was implemented to evaluate the appropriate entrench progression and the LBG algorithm was also implemented to encrypt the data bits in the sub bands coefficients. Finally, the information bits are recuperated from each sub band at the less desirable end. Successive MATLAB simulation demonstrates that the method is sufficiently capable to totally advance the perceptual quality of medical images even after the information has been reconstructed from each sub band at the receiving end.

Further enhancement of medical data confidentiality in future will incorporate embedding in different sub bands of the wavelet transform, since DWT mechanism requires more computational power, more efforts will be done by reducing the computational energy using hybrid optimisation algorithms. Lastly, efforts to provide appropriate and suitable watermarking algorithm to telemedicine clinical scenario is also highly envisaged.

References

Abdulsalam, Y.S., Olaniyi, O.M. and Ahmed, A. (2018) 'Enhanced tiny encryption algorithm for secure electronic health authentication system', *International Journal of Information Privacy, Security and Integrity*, Vol. 3, No. 3, pp.230–252.

Acharya, D. et al. (2011) 'Security in pervasive healthcare networks: current R&D and future challenges', Paper presented at the *11th International Conference on Mobile Data Management*.

Anderson, C.L. and Agarwal, R. (2011) 'The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information', *Information Systems Research*, Vol. 22, No. 3, pp.469–490.

Ben-Assuli, O. (2015) 'Electronic health records, adoption, quality of care, legal and privacy issues and their implementation in emergency departments', *Health Policy*, Vol. 119, No. 3, pp.287–297.

Brifcani, A.M.A. and Brifcani, W.M.A. (2010) 'Stego-based-crypto technique for high security applications', *International Journal of Computer Theory and Engineering*, Vol. 2, No. 6, pp.835–842.

Cao, F., Huang, H. and Zhou, X. (2003) 'Medical image security in a HIPAA mandated PACS environment', *Computerized Medical Imaging and Graphics*, Vol. 27, No. 2, pp.185–196.

Coatrieux, G., Maitre, H. and Sankur, B. (2001) 'Strict integrity control of biomedical images', Paper presented at the *Photonics West 2001 – Electronic Imaging*.

Gabriel, J.A., Alese, K.B., Adetumbi, A.O. and Adewale, O.S. (2013) 'Post-quantum crystography: a combination post-quantum cryptography and steganography', *Proceedings of the IEEE 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, IEEE, USA, pp.449–552.

Guha, S. and Sarmah, D.K. (2015) 'Current status: comparative analysis of optimization techniques used in steganography schemes', *International Journal of Engineering Research in Computer Science and Engineering*, Vol. 2, No. 12, pp.5–11.

Guo, X.C. (2008) *Methodologies in Digital Watermarking: Robust and Reversible Watermarking Techniques for Authentication, Security and Privacy Protection*, University of Toronto.

Hourihan, C. and Cline, B. (2012) *A Look Back: U.S. Healthcare Data Breach Trends*.

IBM (2018) *Cost of Data Breach Study: Global Analysis* [online] https://www.ibm.com/security/data-breach (accessed 2 October 2017).

Kaur, K. and Kaur, E.S. (2016) 'Review of image watermarking technique for medical images', *International Journal of Advanced Research, Ideas and Innovation in Technology*, Vol. 2, No. 5, pp.1–5.

Kumar, N. and Kalpana, V. (2015) 'A novel reversible steganography method using dynamic key generation for medical images', *Indian Journal of Science and Technology*, Vol. 8, No. 16, pp.10–16.

Macq, B. and Dewey, F. (1999) 'Trusted headers for medical images', Paper presented at the *DFG VIII-D II Watermarking Workshop*, Erlangen, Germany, Vol. 10.

Miaou, S.G., Hsu, C.M., Tsai, Y-S. and Chao, H.M. (2000) 'A secure data hiding technique with heterogeneous data-combining capability for electronic patient records', Paper presented at the *Engineering in Medicine and Biology Society*, *Proceedings of the 22nd Annual International Conference of the IEEE*, pp.345–357.

National Health Insurance Scheme (NHIS) (2014) *NHIS Health Insurance Survey Report*, Philips Consulting [online] http://www.phillipsconsulting.net/files/health-insurance-survey-report-jan2014 (accessed 23 July 2017).

Olaniyi, O.M, Arulogun, O.T., Omotosho, A. and Onuh, O.V. (2017) 'Securing clinic tele-diagnostic system using enhanced tiny encrypted radio frequency identification and image steganography technique', *International Journal of Telemedicine and Clinical Practice*, Vol. 2, No. 3, pp.242–266, DOI: 10.1504/IJTMCP.2017.10008683.

Olaniyi, O.M., Folorunsho, T.A., Omotosho, A. and Alegbeleye, I.I. (2015) 'Securing digitized campus clinical healthcare delivery system', *Proceedings of 1st International Conference on Applied Computing (AIT2015)*, Federal University of Agriculture, Abeokuta, Ogun State, pp.18–26.

Rani, M.M. and Lakshmanan, S. (2016) *An Integrated Method of Data Hiding and Compression of Medical Images*, arXiv preprint arXiv: 1604.02797.

Redspin (2011) *Breach Report*, Protected Health Information [online] http://www.redspin.com/docs (accessed 11 March 2016).

Santhi, G. and Adithya, B. (2017) 'A survey on medical image protection using various steganography techniques', *Advances in Natural and Applied Sciences*, Vol. 11, No. 12, pp.89–95.

Saxena, A.K., Sinha, S. and Shukla, P. (2018) 'Design and development of image security technique by using cryptography and steganography: a combine approach', *International Journal of Image, Graphics & Signal Processing*, Vol. 10, No. 4, pp.223–230.

Shaik, A., Thanikaiselvan, V. and Amitharajan, R. (2017) 'Data security through data hiding in images: a review', *Journal of Artificial Intelligence*, Vol. 10, No. 1, pp.1–21.

Shikha and Dutt, V.K. (2014) 'Steganography: the art of hiding text in image using MATLAB', *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 4, No. 9, pp.7–15.

Singh, P. and Chadha, R. (2013) 'A survey of digital watermarking techniques, applications and attacks', *International Journal of Engineering and Innovative Technology*, Vol. 2, No. 9, pp.165–175.

Solichin, A. and Ramadhan, E.W. (2017) 'Enhancing data security using DES-based cryptography and DCT-based steganography', in *Science in Information Technology (ICSITech), 3rd International Conference*, IEEE, pp.618–621.

Symantec (2013) *Cost of Data Breach Study: Global Analysis* [online] https://www.symantec.com/mktginfo/whitepaper (accessed 23 July 2017).

Trichili, H., Boublel, M., Derbel, N. and Kamoun, L. (2002) 'A new medical image watermarking scheme for a better telediagnosis', Paper presented at the *2002 IEEE International Conference on Systems, Man and Cybernetics*, pp.234–245.

Vallathan, G., Devi, G.G. and Kannan, A.V. (2016) 'Enhanced data concealing technique to secure medical image in telemedicine applications', Paper presented at the *Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference*, pp.678–685.