Original Research Article

A Hybrid Cryptosystem and Watermarking for Secure Medical Image Transmission

ABSTRACT

Advances in computing and communication technologies have provided new methods to store and access medical data electronically and distribute them over open communication networks. Today, patients themselves can access their medical information themselves and medical information can be transmitted among medical institutions as well as stockholders in the health sector. Accompanying these benefits are concomitant risks for patient medical record in electronic formats and strictly personal medical documentation being transmitted and accessible over open communication channels such as the Internet. Thus it is common knowledge that there should be in place network-level security measures and protocols in medical information systems. Many security schemes that were based on cryptography, watermarking and steganography have been proposed and implemented to secure medical data. However, an apt review of relevant literature revealed in many implementations robustness against attacks is not guaranteed. Issues bordering on low embedding capacity, low robustness, low imperceptibility and bad trade tradeoff between robustness and capacity are evident in many implementations. In this paper, a hybrid Rivest-Shamir-Adleman (RSA) algorithm, Rivest Cipher 4 (RC4) algorithm and Spread Spectrum techniques were proposed for securing medical image data over open communication networks. The performance of the proposed scheme was evaluated using Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR), Mean Square Error (MSE) and Bit Error Rate (BER). For the five sample medical images used to test the scheme, the BER value is zero while the PNSR and SNR are consistent and they returned desirable high values. The MSE values for the images are low. The average values of the PSNR, SNR and MSE are 51.88 dB, 43.38 dB and 0.113 respectively. Hence, the proposed scheme is utterly revertible, robust and highly imperceptible; the original images can be retrieved by the recipient without any deformation or alteration.

Keywords: Cryptography, Medical Image, Watermarking, Rivest Cipher 4, Rivest-Sharmir-Adleman, Security, Spread Spectrum

1. INTRODUCTION

One of the most outstanding innovative developments that came by the way of information and communications technology (ICT) is the Internet. Almost every facet of our human life has felt the impact of the widespread accessibility, adaptability and applications of ICT. The healthcare sector is not an exemption. One essential application of the Internet in the healthcare sector is the transmission of medical information as Electronic Patient Records (EPR) among medical institutions, which has become very prominent nowadays ([1]; [2]; [3]; [4]). EPR typically contain the health history of a patient, including demographic data, physical examinations, laboratory tests, treatment procedures, prescriptions, radiology examinations, historic pathology, to mention but a few [5]. The format of an EPR can be presented in various templates such as diagnostic reports, images, vital sign signals and so

on. An EPR transmitted through the Internet is especially important since it contains highly private contents of medical information for a person. Hence, the disclosure of an EPR would not only discomfit the concerned individual but may also be accompanied by unexpected losses which may be physical or financial.

To every coin, there are two sides. As the advances in computing and communication technologies came with its value-added advantages, so also are its attendant problems. Technological advancements have eased the replication, manipulation and unauthorized distribution of the medical data [5], resulting in the precondition for protection from unauthorized access and preservation of the integrity of medical data [6]. In exchanging medical data over an open network, of utmost importance is the requirement for confidentiality, the protection of the copyright and authentication of the contents of such data ([7]; [8]; [9]; [10]). In medical imaging, the digital imaging and communication in medicine (DICOM) provides the basic mechanism to exchange the medical image data via the open channel ([11]; [12]). However, a header attached with DICOM images may be attacked, hacked or lost, resulting in the insecure transmission ([13]; [14]).

In proffering solution to these problems, there are two major techniques: one is encryption, and the other one is information hiding. As a conventional solution of secure communication on insecure channels, encryption has been extensively investigated ([15]; [16]; [17]; [18]; [19]; [20]; [21]; [22]; [23]), and many encryption models have been proposed to provide confidentiality, availability and reliability based on the outcomes of information integrity and authenticity. On the other hand, with the improvement in data hiding and digital watermarking technologies, many schemes have been proposed to embed information into medical images ([17]; [24]; [25]) for the protection of confidential information and the authentication of medical data. Both encryption and data hiding have their strengths in secure communication; hence the integration of encryption and digital watermarking is considered as the best approach for enhanced protection of medical images and data thereby protecting them against abuse and illicit circulation ([26]; [27]). Many security schemes that were based on either encryption or watermarking or a combination of both have been proposed and implemented to secure medical data. However, an apt review of relevant literature revealed in many implementations robustness against attacks is not guaranteed. Issues bordering on low embedding capacity, low robustness, low imperceptibility and bad trade tradeoff between robustness and capacity are evident in many implementations; hence making them susceptible to attacks.

A security scheme for ensuring the aforementioned information security requirements for medical images transmitted over open communication channels is proposed in this paper. Medical images are a central part of diagnostics in today's healthcare delivery [57]. Medical imaging includes diverse imaging techniques and procedures to pictorially represent the human body for diagnostic and treatment purposes. The significance of these images is also evident in the assessment of an ailment/syndrome previously diagnosed and/or treated. In today's medicine, these images are digitized; moreover, often they are exchanged through open communication channels. In this paper, a hybrid RSA-RC4 algorithm and spread spectrum techniques are proposed for securing medical images. RC4, a private key cypher, was used for image encryption while RSA, a public key cypher was used to encrypt the secret key of RC4. The encrypted secret key of RC4 was hidden in the encrypted image using a combination of Direct Sequence Spread Spectrum (DS-SS) and Frequency Hopping Spread Spectrum (FH-SS) techniques. Section two presents review of relevant literature to this research; Section three details the research methodologies employed in the development of the security scheme; Section four presents the results and section five summarized and concludes the paper.

2. LITERATURE REVIEW

2.1 Medical Images Transmission and Security Concerns

Nowadays, medical imaging has become a major part of the most diagnostic process. According to (Rey and Dugelay, 2002) in [28], medical images play a major role for instantaneous diagnosis, understanding of key diseases as well as to avoid the wrong diagnosis in the telemedicine, telediagnosis and tele-consultancy services. Medical images are the most integral element of most healthcare diagnostic procedures because they are used to observe and analyse characteristic attributes of patients which may include anatomical cross-sections of internal organs and tissues. Furthermore, they are essentials utilized by medical practitioners to assess the patient's diagnosis and examination of the outcome of the treatment. Therefore, providing access control for medical images is a crucial requirement. Fotopoulos *et al.* in [24] subscribed that medical images used for diagnosis are required to be secured to forestall malevolent modification because most time, they are closely related to patients' privacies and hence should be kept with utmost secrecy.

In essence, medical images, as a matter of basic necessity must be kept confidential. The transmission of medical images over open communication channels necessitates an integrity check with the intent of ensuring quality control: actuality (instantaneous precision in the interest of the information) and reliability (verification of the source and integrity). Security of medical images, which came by the way of strict ethics and legislative rules, gives rights to the patient and duties to the medical professionals. This compels the satisfaction of the three obligatory characteristics; that is confidentiality, reliability and availability ([2]; [29]).

i. confidentiality means that only the entitled users, under the defined terms, have access to the information:
ii. reliability which is of two perspectives;
    a) Integrity: the information content has not been modified, forged, deleted without detection, and,
    b) Authentication: a verification that the ownership of information is actually due to the right patient and it emanated from the expected source;
iii. availability is the capacity of an information system to be used by the entitled users under the defined terms of access and exercise.

2.2 Cryptography

Cryptography is the science of ensuring secrecy of secrets [30]. The initial message from the sender's side is referred to as the plaintext, while the encoded message sent to the receiver is called the ciphertext. The procedure of translating from the plaintext to ciphertext is called enciphering or encryption while reinstating the plaintext from the ciphertext is termed deciphering or decryption; a cypher is a two-way algorithm that initiates the encryption and the reversing decryption [31]. The fundamental and classical task of cryptography is to provide confidentiality by encryption methods. Providing confidentiality is not the only objective of cryptography. Cryptography is also used to provide solutions for other information security problems [30]:

i. *Data integrity*. The receiver of a message should be able to check whether the message was modified during transmission, either accidentally or deliberately. No one should be able to substitute a false message for the original message, or parts of it.
ii. *Authentication*. The receiver of a message should be able to verify its origin.
iii. *Non-repudiation*. The sender should not be able to later deny that he/she sent a message.

Generally, there are three types of streams in cryptography: symmetric key, asymmetric key and hashing. Symmetric-key cryptography uses a single secret key for both encryption and decryption purpose. The implementation of Secret key cyphers is as either block cyphers or stream cyphers. The former encrypts input in blocks of plaintext instead of individual characters, the input form as obtained in stream cyphers [32]. Data manipulation in symmetric cypher is faster as they generally use shorter key lengths. One major disadvantage of the secret key cypher is the key management required for their security applications. Every unique pair of parties that wants to communicate needs to share different keys and possibly for every ciphertext exchanged too. The total number of keys needed is proportional to the square of the number of network members, which rapidly requires composite key management systems to store them reliably and confidentially [31]. Examples of symmetric-key encryption algorithm are AES, Data Encryption Standard (DES), Triple DES (3DES), RC4 to mention but a few.

On the other hand, asymmetric key cryptography uses two keys: one is the public key and another one is the private key. Receiver's public key is used by the sender for encrypting the message and receiver's private key is used for decrypting the message at the receiver. Producing such keys depends on cryptographic algorithms based on mathematical problems to generate one-way functions. Efficient security involves keeping the private key private while the public key can be explicitly shared without security concession [31]. In public-key encryption, a message is encrypted by anyone using the receiver's public key, however, the encrypted message can only be decrypted with the receiver's private key [30]. Public key algorithms are fundamental security ingredients in modern cryptosystems, applications and protocols assuring the confidentiality, authenticity and non-reputability of electronic communications and data storage. Example of this class of encryption algorithm includes RSA, Diffie–Hellman key exchange protocol, Elliptic curve techniques, El-Gamal to mention but a few.

2.2.1 RSA Algorithm

RSA utilizes an expression with exponentials. The RSA algorithm encrypts the plaintext in blocks, with each block having a binary value less than a certain number n. In another word, the value of the block size must be less than or equal to $\log_2(n) + 1$; in practice, the block size is i bits, where $2^i < n \leq 2^{i+1}$. The encryption and decryption processes of the algorithm follow the format, for some plaintext block M and ciphertext block C [31]:

$C = M^e \bmod n$ 2.1

$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public key encryption algorithm with a public key of $PU = \{e, n\}$ and a private key of $PR = \{d, n\}$. For this algorithm to be satisfactory for public-key encryption, the following requirements must be met [58].

i. It is possible to find values of e, d, and n such that $M^{ed} \bmod n = M$ for all $M < n$.
ii. It is relatively easy to calculate $M^e \bmod n$ and $C^d \bmod n$ for all values of $M < n$.
iii. It is infeasible to determine d given e and n.

The first requirement is to find a relationship of the form:

$M^{ed} \bmod n = M$ 2.2

The preceding relationship holds if e and d are multiplicative inverses modulo $\varphi(n)$, where $\varphi(n)$ is the Euler totient function. For p, q prime, $\varphi(pq) = (p - 1)(q - 1)$. The relationship between e and d can be expressed as

$ed \bmod \varphi(n) = 1$ 2.3

This is equivalent to saying

$ed \equiv 1 \bmod \varphi(n)$

$d \equiv e^{-1} \bmod \varphi(n)$

That is, *e* and *d* are multiplicative inverses mod φ(*n*). It may be noted that, according to the rules of modular arithmetic, this is true only if *d* (and therefore *e*) is relatively prime to φ(*n*).
Equivalently, gcd(φ(*n*), *d*) = 1. 2.4
In summary, the essential ingredients of the RSA scheme are:
p, q, two prime numbers (private, chosen)
n = *pq* (public, calculated)
e, with gcd(φ (*n*), *e*) = 1; 1< *e* < φ(*n*) (public, chosen)
$d \equiv e^{-1} \pmod{\varphi(n)}$ (private, calculated)
The private key consists of {*d*, *n*} and the public key consists of {*e*, *n*}. Suppose that user A has published its public key and that user B wishes to send the message *M* to A. Then B calculates $C = M^e \bmod n$ and transmits *C*. On receipt of this ciphertext, user A decrypts by calculating $M = C^d \bmod n$.

2.2.2 RC4 Algorithm

RC4 is a binary additive stream cypher [33]. It uses a variable-sized key that can range between 8 and 2048 bits in multiples of 8 bits (1 byte). This means that the core of the algorithm consists of a keystream generator function. This function generates a sequence of bits that are then combined with the plaintext with XOR. Decryption consists of regenerating this keystream and "XORing" it to the ciphertext, undoing it. The other major part of the algorithm is the initialization function, *n* which accepts a key of variable size and uses it to create the initial state of the keystream generator. This is also known as the key schedule algorithm [34].

RC4 is a class of algorithms parameterized on the size of its block. This parameter, *n*, is the word size for the algorithm. It is recommended that *n = 8*, but for analysis purposes, it can be convenient to reduce this. Also, for extra security, it is possible to increase this value. The internal state of RC4 consists of a table of size 2^n words and two words sized counters. The table is known as the S-box and will be known as *S* [35]. It always contains a permutation of the possible 2^n values of a word. The two counters are known as *i* and *j*.

The Key Schedule Algorithm of RC4 is depicted as follows:
$\boldsymbol{Initialization}$:
$For\ i = 0\ to\ 2^n - 1$
$S[i] = i$
$j = 0$
$\boldsymbol{Scrambling}$:
$For\ i = 0\ to\ 2^n - 1$
$j = j + S[i] + K[i\ mod\ l]$
$Swap(S[i], S[j])$
It accepts as input the key stored in *K*, and is l bytes long. It starts with the identity permutation in *S* and, using the key, continually swapping value to produce a new unknown key-dependent permutation. Since the only action on S is to swap two values, the fact that *S* contains a permutation is always maintained. The RC4 keystream generator algorithm is as follows:
$\boldsymbol{Initialization}$:
$i = 0$
$j = 0$
$\boldsymbol{Generation\ Loop}$:
$i = i + 1$
$j = j + S[i]$
$Swap(S[i], S[j])$
$Output\ z = S[S[i] + S[j]]$

It works by continually shuffling the permutation stored in *S* as time goes on, each time picking a different value from the *S* permutation as output. One round of RC4 outputs an *n* bit word as keystream, which can then be XOR'ed with the plaintext to produce the ciphertext.

2.3 Digital Watermarking

The proliferation of digitized media which could be audio, image or video is creating an imperative need for copyright enforcement schemes that protect copyright ownership [36]. Traditional cryptosystems allow only authorised keyholders access to encrypted data, but once such data is decrypted there is no way to track its reproduction or retransmission. Consequently, traditional cryptography provides modest security against data piracy, in which a publisher is confronted with unauthorized reproduction of information. A digital watermark is intended to complement cryptographic processes. It is a visible, or preferably invisible, identification code that is permanently embedded in the data and remains present within the data after any decryption process. Digital Watermarking is a technology of embedding watermark with intellectual property rights into images, videos, audios and other multimedia data by a certain algorithm [37; 38].

A watermark should have the characteristics outlined below [36]:

i. *Unobtrusiveness:* The watermark should be perceptually invisible, or its presence should not interfere with the work being protected.
ii. *Robustness:* The watermark must be difficult (hopefully impossible) to remove. If only partial knowledge is available (for example, the exact location of the watermark in an image is unknown), then attempts to remove or destroy a watermark should result in severe degradation in the fidelity before the watermark is lost.
iii. *Universality:* The same digital watermarking algorithm should apply to all three media under consideration. This is potentially helpful in the watermarking of multimedia products. Also, this feature is conducive to the implementation of audio and image/video watermarking algorithms on common hardware.
iv. *Unambiguousness:* Retrieval of the watermark should unambiguously identify the owner. Furthermore, the accuracy of owner identification should degrade gracefully in the face of attack.

2.3.1 Spread Spectrum Techniques

In digital watermarking, the watermark should not be placed in perceptually insignificant regions of an image (or its spectrum), since many common signal and geometric processes could affect these components. The problem then becomes how to insert a watermark into the most perceptually significant regions of the spectrum in a fidelity preserving fashion. Any spectral coefficient may be altered, provided such modification is small. However, very small changes are very susceptible to noise. To solve this problem, the frequency domain of an image at hand can be viewed as a communication channel, and correspondingly, the watermark is viewed as a signal that is transmitted through it. Attacks and unintentional signal distortions are thus treated as noise that the immersed signal must be immune to. In spread spectrum communications, one transmits a narrowband signal over a much larger bandwidth such that the signal energy present in any single frequency is undetectable. Similarly, the watermark is spread over many frequency bins so that the energy in any one bin is very small and certainly undetectable. The mostly described spread spectrum techniques DS-SS and FH-SS techniques [39].

In the DS-SS algorithm, a low-level wideband signal can be easily hidden within the same spectrum as a high power signal, which each signal appears to be noise to the other. The core component of these spread spectrum systems is a Pseudo-Random Noise Sequence

(PRNS). For these direct sequence spread spectrum systems, the original baseband bitstream is multiplied by the PRNS to produce a new bitstream [40]. Only those receivers equipped with correct PRNS can decode the original image. At the receiver, the low-level wideband signal will be accompanied by noise. By using a suitable detector with the correct PRNS, this signal can be squeezed back into the original narrow baseband. As the noise is completely random and uncorrelated, the desired signal can easily be extracted.

The FH-SS algorithm involves a periodic change of transmission frequency. A frequency hopping signal may be regarded as a sequence of modulated data bursts with time-varying, pseudo-random carrier frequencies. The set of possible carrier frequencies is called the hopset. Hopping occurs over a frequency band that includes several channels. Each channel is defined as a spectral region with a central frequency in the hopset. The bandwidth is large enough to include most of the power in a narrow band modulation burst, having the corresponding carrier frequency. Data is therefore sent by hopping the transmitter carrier to seemingly random channels which are known only to the desired receiver. On each channel, small bursts of data are sent using conventional narrowband modulation before the transmitter hops again.

A. Watermark Embedding

In the DS-SS algorithm, a sequence of information bits, consisting of “-1” and “1”, is spread by multiplying with a large factor, called the chip-rate C_r, to obtain the spread information sequence. The size of this sequence is equal to the value of chip-rate multiplied by the number of information bits. The spread sequence is then modulated with a binary pseudo-noise sequence to yield the modulated spread sequence and is finally amplified with a locally adjustable amplitude factor to obtain the watermark signal.

Each bit of the watermark signal will be embedded into some assigned locations, which is randomly determined by a key-based FH-SS technique, within the image frame, instead of the whole frame. Therefore, each watermark bit will only be dispersed over its corresponding locations within some parts of the image. Each watermark bit is merely embedded into the assigned pixels by using additive operation. The output will be the watermarked pixels. This ratio is up to the applications and the user's satisfaction. Furthermore, in the proposed scheme, only some of the selected pixels will be used to carry the watermark signal.

B. Watermark Extraction

To recover the embedded information, it is necessary to precisely determine the hopping locations, where the watermark signal is added. The watermarked pixels are firstly correlated with the same pseudo-noise sequence used in the generating process. The correlation here is performed by demodulation followed by summation over the width of the chip-rate. Finally, the sign of the correlation sum determines the embedded information bit.

2.4 Related Works

Tolbal *et al.*, in [41] proposed a wavelet transform algorithm that maps integers to integers for perfect reconstruction of the original image. The proposed algorithm embeds the message bitstream into the LSB's of the integer wavelet coefficients of a true-colour image. The algorithm also applies a pre-processing step on the cover image to adjust saturated pixel components to recover the embedded message without loss.

Boucherkha and Benmohamed in [42] presented a medical image authentication based on lossless watermarking; it is used for interleaving patient information and message authentication code with images using lossless compression. At the embedding process, the authentication code of the image using MD5 algorithm is calculated; the authentication code

and patient information are concatenated then encrypted. LSBs of all pixels are selected and compressed using Run Length Encoding (RLE) lossless compression algorithm. The compressed string and the encrypted string are concatenated and inserted into the LSB locations by adding blanks if necessary. Before embedding process the patient information is encrypted; therefore, this technique provides a high level of security for the patient information. This presented technique inherits the disadvantage of the LSB embedding process that is changing the statistical property of the cover image; therefore, the hiding process can be detected easily by computer systems.

Delforouzi and Pooyan in [43] presented a novel method for digital audio steganography in which encrypted covert data is embedded into the coefficients of the host audio (cover signal) in the integer wavelet domain. The hearing threshold is calculated in the integer domain and this threshold is employed as the embedding threshold. The inverse integer wavelet transform is applied to the modified coefficients to form a new audio sequence (stego signal).

Memon and Gilani in [44] proposed an adaptive data hiding scheme for medical images using integer wavelet transform. Integer wavelet transform hiding technique is used for embedding the multiple watermarks by decomposes the cover image to obtain the wavelet coefficients. Before watermark embedding process; an adaptive threshold is determined for each block; it uses iterative optimization of the threshold for compression and expansion process. It avoids histogram pre and post-processing; therefore, its pros are reducing the histogram processing overhead and keeping the distortion small between the watermarked and the original images. The cons of this technique are low imperceptibility values at normal embedding capacity (bad tradeoff between robustness and capacity) and it is not applied to colour images (it is applied only for grayscale images).

Luo *et al.*, in [45] presented a scheme embeds a larger-sized secret image while maintaining acceptable image quality of the stego-image and also improved image hiding scheme for grayscale images based on Integer wavelet transformation.

Mostafa *et al.* in [46] proposed a blind watermarking based on wavelet transform for medical image management, it hides the Electronic Patient Record (EPR) in the image: to protect patient information, to save storage space and to reduce transmission overheads. It embeds EPR data as a watermark in the Discrete Wavelet Packet Transform (DWPT) of the image. This proposed technique enhances the robustness by encoding EPR data using BCH error-correcting code. The disadvantages of this technique are that it is purely implemented for grayscale images (not for colour images), and it has been low embedded capacity. The embedded process hides only one bit per a block of pixels with size 4×4 pixels, and the error-correcting code reduces the actual capacity to be less than one bit per 4×4 block of pixels.

Memon in [47] presented a robust fragile watermarking technique to provide copyright protection and content authentication of medical images. It authenticates the CT scan images of the thorax area against distortions. It separates a ROI and RONI from the image. By isolating the actual lung parenchyma; this technique increases the embedding capacity of a CT scan image; it embeds a watermark only in RONI; therefore, it does not compromise the diagnostic value of the image. For embedding the watermark; it utilizes the spatial domain watermarking and LSB replacement method. The cons of this technique are it is devoted to a specific type of medical images; also, its robustness requires to be improved.

Sakkara *et al.*, in [48] proposed a technique that uses secret information as a text message which is embedded in a colour image. The technique is founded around the fact that most

existing methods hide the information using a constant bit length in integer wavelet coefficients that increases the embedding capacity of the text message and obtained stego image is imperceptible for human vision.

Ko *et al.*, in [49] proposed a reversible watermark based on Quantization Index Modulation (QIM) to be applied to healthcare information management systems, the QIM-based watermarking is used to reconstruct the identical original image; the capacity of the watermark is increased to be one-fourth of that of the cover image. Its architecture and algorithms are simple; it can be easily implemented. However, it is tested using only grayscale images; accordingly, it is required to be tested using colour images.

Pandey, Singh and Shrivastava in [50] presented a security model that combines image cryptography, data hiding and Steganography technique for denoised and safe image transmission purpose. In the model, the original images are encrypted with the stream cypher algorithm then embeds the encrypted image with patient information by using lossless data embedding technique with data hiding key after that for more security. Steganography is then applied to the embedded image with the private key. On receiver side when the message arrives the methods are applied in reverse order to get the original image and patient information and to remove noise we extract the image before the decryption of the message.

An *et al.,* in [51] proposed a watermarking framework based on wavelet-domain; it proposes a robust reversible watermark embedding and extraction procedure through histogram shifting and clustering. It provides good performance in terms of reversibility, robustness and invisibility, but the embedded capacity is less than 4×10^{-3} bpp. It is applicable in practice to many types of medical images; however, it is tested using a limited number of grayscale images; therefore, it is required to be tested using enough number of grayscale and colour images.

Das and Kundu in [52] proposed a blind image watermarking technique based on Contourlet (CN) transform for the medical data-management scheme. It is robust against high JPEG and JPEG2000 compression, and it can provide information security, content authentication, safe archiving and controlled access retrieval. In this proposal, an original image is decomposed based on CN transform, then the watermark is embedded inside the image using the low pass such that the embedded watermark can be extracted blindly, finally the image is reconstructed based on the inverse of the CN transform to get the watermarked image. It can be used during a medical image acquisition process to provide authenticity, integrity and confidentiality, but the embedded capacity is very low it is less than 0.0053 bpp.

Bouslimi, Coatrieux and Roux in [53] proposed a security technique based on encryption, and watermarking to protect medical images; it enables access to the outcomes of the encrypted image integrity and its origins. With this technique, the RC4 stream cyphers and two substitute watermarking methods are combined; these two watermarking methods are the LSB and the QIM methods. In the embedding process, the watermarking and encryption are conducted jointly; therefore, in the extraction process, the watermark extraction and decryption can be applied independently. This technique can achieve a large embedded capacity in the spatial domain (0.5 bpp) with a high Peak Signal to Noise Ration (PSNR) that is greater than 49 dB. Due to using the LSB watermarking method; the statistical property of the watermarked images is changed; accordingly, the hidden information can be detected by the attacking -computer system.

Jain, Choudhary and Kumar in [54] presented a novel technique for securing the transmission of medical information of patient inside the medical cover image by concealing

data using decision tree concept. The decision tree shows a robust mechanism by providing decisions for secret information concealing location in medical carrier image using secret information mapping concept. RSA encryption algorithm was used for the patient's unique information enciphering. The outcome of the RSA was structured into various equally distributed blocks.

Mahalakshmi, Satheeshkumar and Sivakumar in [55] proposed a security model for protecting medical images with emphasis on Magnetic Resonance Imaging (MRI). In their work, three different steganographic algorithms were used; Least Significant Bit (LSB) algorithm, Division into the block and Mean change modified method.

Banjan and Dalvi in [56] presented a medical data security model using a combination of cryptography and steganography with AES-LSB algorithm. In the model, patient's data is firstly encrypted using the Advanced Encryption Standard algorithm and then the encrypted data is hidden in a medical image using image steganography by Least Significant Bits algorithm. The hidden data in the cover image is sent to the intended receiver. The reverse of the process is used to obtain the original data at the receiver side.

The review of the above-mentioned literature revealed that many security schemes proposed for securing medical images still contends with issues bordering on low embedding capacity, low robustness, low imperceptibility and bad trade tradeoff between robustness and capacity and hence making them susceptible to attacks.

3. METHODOLOGY

The use of computer networks for data transmissions has created the need for security. Many robust message encryption techniques have been developed to supply this demand. The encryption process can be symmetric, asymmetric or hybrid and can be applied to blocks or streams. Several asymmetric algorithms use long keys to ensure confidentiality because a part of the key is known. These algorithms are not appropriate enough to be applied to images because they require a high computational complexity. In the case of block encryption methods applied to images, one can encounter three inconveniences. The first one is when there are homogeneous zones (regions with the same colour); all blocks in these zones are encrypted in the same manner. The second problem is that block encryption methods are not robust to noise. Indeed, because of the large size of the blocks (which is at least 128 bits) the encryption algorithms per block, symmetric or asymmetric, cannot be robust to noise. The third problem is data integrity. Hence the adoption of a stream cypher in the RC4 for encryption.

The proposed security scheme can be discussed as follows: Assuming *X* wishes to send a medical image securely over an open communication channel to *Y. X* will use RC4 to encrypt the medical image. However, *X* must initially generate a secret key to encrypt medical mage. The secret key will then be encrypted with the RSA public key. The encrypted private key of RC4 will then be embedded into the encrypted image using DS-SS and FH-SS techniques. The encrypted watermarked image is afterwards transmitted over an open network to *Y*. On reception of the encrypted watermarked image by *Y*, the watermark, that is, the encrypted secret key of RC4 is extracted and then decrypted with RSA private key. The evolving decrypted secret key of RC4 is then used by *Y* to decrypt the image to retrieve the original medical image. The architecture framework of the security scheme is depicted in Fig. 1.

Algorithmic representation of the proposed security scheme is highlighted as follows:

i. Create an RSA key pair; a private key and a public key.

ii. *Generate a random secret key for RC4.*
iii. *Create an RC4 cypher to encrypt the image with the RC4 secret key.*
iv. *Encrypt the image with the RC4 key.*
v. *Encrypt the RC4 key with the RSA public key.*
vi. *Using DS-SS/FH-SS algorithms, embed the encrypted RC4 key as a watermark into the encrypted image.*
vii. *Transmit the encrypted watermarked image.*
viii. *At the recipient's end, extract the watermark from the encrypted watermarked image.*
ix. *Decrypt the RC4 key using the RSA private key.*
x. *Use the RC4 key to decrypt the encrypted image to read the original image.*

The RSA, RC4 and DS-SS/FH-SS algorithms have been aptly described in Section Two of the paper. An application was developed using Microsoft Visual Studios(C# Programming Language) and MATLAB R2016a environment to implement the scheme. The main application and user interfaces were developed using C# Programming Language, and they call MATLAB functions to read and write the sample medical images used to experiment with the scheme. The evaluation parameters used to measure the performance of the proposed scheme are Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR), Mean Square Error (MSE) and Bit Error Rate (BER).

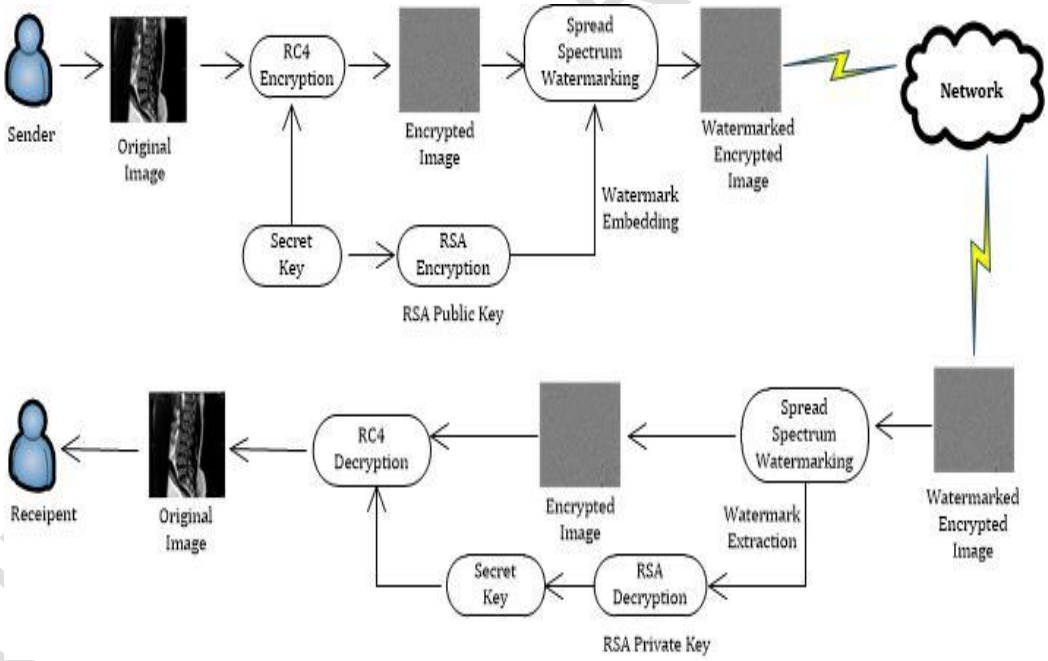

Fig. 1. Architectural Framework of the Proposed Security Scheme

4. RESULTS AND DISCUSSION

The proposed security scheme was applied to five grayscale sample medical images (512 x 512 pixels). The original image, encrypted image, key extracted image and decrypted images of one the sample images used are presented in Fig. 2A, 2B, 2C and 2D respectively.

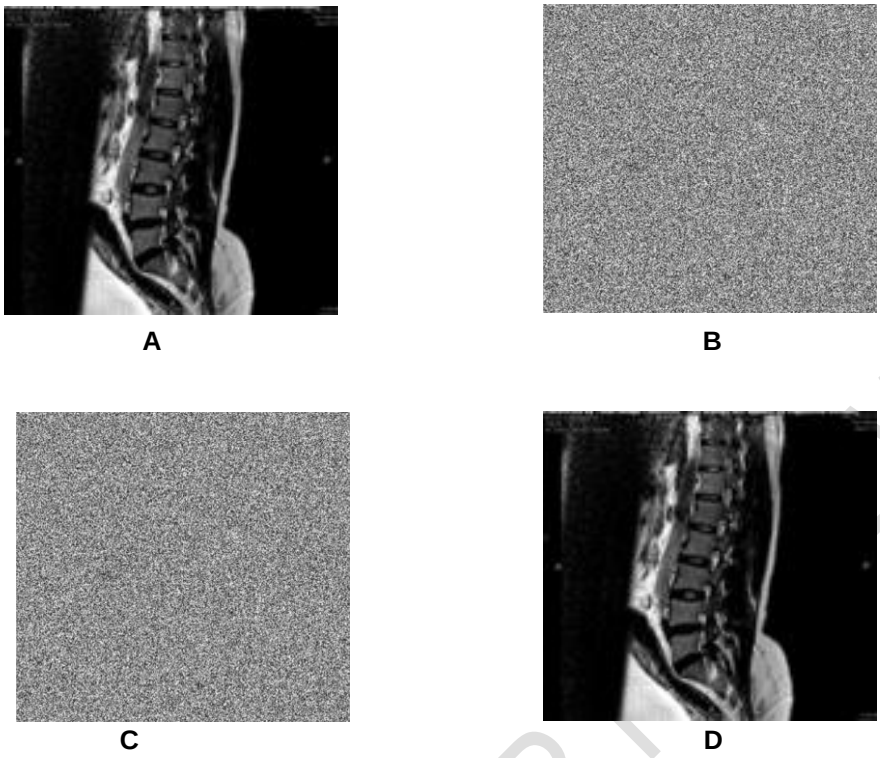

Figure 2: Original, Encrypted, Watermarked, Key Extracted and Decrypted Images of a Sample Medical Image

Using the human visual system to detect differences between the original image and decrypted image of Figure 2 no one can detect the difference between them; therefore, proving the efficacy of the proposed scheme. Table 1 details the results of the performance parameters used in evaluating the efficiency of the proposed security scheme. Summarily, these results proved that the proposed scheme is utterly revertible, robust and highly imperceptible; the original images can be retrieved at the receiver side without any distortion.

From Table 1, the PSNR has large consistent values; the minimum value is 51.42 dB while the highest value is 52.37 dB. These large values of PSNR (that is > 36 dB) indicate that distortion due to encryption and embedding of a watermark in the original image is very low; the encryption and the embedded watermark and did not affect the quality of the original images, and the identical original image can be extracted at the receiver side.

The minimum value of SNR is 41.98 dB; this, consequently, indicates that the SNR has desirable values; therefore, corruption due to embedding the watermark in the original image is very low. The maximum value of MSE is 0.121; an indication that the MSE has very low consistent value; therefore, the embedded watermark does not affect the quality of the original images. The BER value is zero for all five images, an indication that the bitstream sequence extracted from the image at the receiver side is identical to the bitstream sequence embedded in the image at the sender side.

Table 1: Results of Performance Evaluation Parameters

Sample	PSNR	SNR	MSE	BER

Medical Image	(dB)	(dB)		(%)
SM_Image1	51.76	44.28	0.115	0
SM_Image2	51.42	42.83	0.121	0
SM_Image3	52.16	41.98	0.109	0
SM_Image4	51.68	43.24	0.118	0
SM_Image5	52.37	44.56	0.102	0

5. CONCLUSION

With the development of advanced technologies in computer networks and communication field, the transmission of medical information among medical institutions has become more prominent nowadays. However, the technological advancements have eased the duplication, manipulation and unauthorized distribution of the medical data, resulting in the prerequisite for protection from unauthorized access and maintaining the integrity of medical data.

In this paper, a hybrid RSA-RC4 algorithm and spread spectrum techniques were proposed for securing medical images. RC4, a private key cypher, was used for image encryption while RSA, a public key cypher was used to encrypt the secret key of RC4. The encrypted secret key of RC4 was hidden in the encrypted image using a combination of Direct Sequence Spread Spectrum (DS-SS) and Frequency Hopping Spread Spectrum (FH-SS) techniques. The performance evaluation of the proposed scheme showed that utterly revertible, robust and highly imperceptible; the original images can be retrieved at the receiver side without any distortion.

The direction of future work can be tuned to practically including the proposed technique within Health Information Systems to provide medical image integrity, system authentication and confidentiality.

REFERENCES

[1] Matheson L. R., Mitchell S. G., Shamoon T. G., Tarjan R. E. and Zane F**.** - Robustness and Security of Digital Watermarks", Financial Cryptography, Lecture Notes in Computer Science, 1465: pp. 227-240, 1998.

[2] Coatrieux G., Maitre H., Sankur B., Rolland Y., and Collorec R. - Relevance of Watermarking in Medica Imaging. In: Proc. IEEE Conference on Information Technology Applications in Biomedicine, Arlington, USA, pp. 250-255, 2000.

[3] Mohanty S. P. - Digital Watermarking: A Tutorial Review. The report, Indian Institute of Science, India, 2000.

[4] Coatrieux G., Lecornu L., Roux C. H. Sankur B. - A Review of Image Watermarking Applications in Healthcare. In: Proc. of 28th Annual International Conference Engineering in Medicine and Biology Society, EMBS '06, IEEE, New York, pp.4691-4694, 2006.

[5] Chao H-M., Hsu C-M. and Miaou S-G., - A Data-hiding Technique with Authentication, Integration and Confidentiality for Electronic Patient Records. IEEE Transactions on Information Technology in Biomedicine, 6(1): 46-53, 2002.

[6] Singh A. K, Kumar B., Dave M. and Mohan A., - Multiple Watermarking on Medical Images Using selective DWT Coefficients. Journal of Medical Imaging and Health Informatics, 5(3): 607-614, 2015.

[7] Acharya R., Bhat P. S., Kumar S. and Min L. C. - Transmission and Storage of Medical Images with Patient Information. Computers in Biology and Medicine, 33(4): 303-310, 2013.

[8] Giokoumaki A., Pavlopoulos S. and Koutsouris D. - Secure and Efficient Health Data Management through Multiple Watermarking on Medical images. Journal of Medical and Biological Engineering and Computing, 44(8):619-631, 2006.

[9] Lavanya A. and Natarajan V., Watermarking Patient Data in Encrypted Medical Images. Sadhana, 37(6):723-729, 2012.

[10] Singh A. K., Dave M. and Mohan A., - Multilevel Encrypted Text Watermarking on Medical Images Using Spread-spectrum in DWT Domain. Wireless Personal Communications, 83(3): 2133-2150, 2015.

[11] Mildenberger P., Eichelberg M. and Marthin E. - Introduction to the DICOM Standard. European Radiology, 12(4): 920-927, 2002.

[12] Cao F., Huang H. K. and Zhou X. Q., - Medical Image Security in a HIPAA Mandated PACS Environment. Computerized Medical Imaging and Graphics, 27(2): 185-196, 2003.

[13] Rati O. and Rosset A., - " Open-source Software in Medical Imaging: development of OsiriX. International Journal of Computer Assisted Radiology and Surgery, 1(4):187-196, 2006.

[14] Lu X., Zhang M., Yang L., Zhao Y. and Liu J. - Research and Implementation of Medical Images Management System Based on DICOM Standard. International Conference on Biological and Biomedical Sciences, Newark, United States, 9: 140-160, 2012.

[15] Gao T. and Chen Z., - A New Image Encryption Algorithm Based on Hyper-chaos," Physics Letters A, 372(4):394–400, 2008.

[16] Zhang X.,- Separable Reversible Data Hiding in Encrypted Image, IEEE Transactions on Information Forensics and Security, 7(2):826–832, 2012.

[17] Bouslimi D., Coatrieux G., Cozic M., and Roux C. - A Joint Encryption /watermarking System for Verifying the Reliability of Medical Images, IEEE Transactions on Information Technology in Biomedicine, 16: 891–899, 2012.

[18] Francois M., Grosges T., Barchiesi D. and Erra R. - A New Image Encryption Scheme Based on a Chaotic Function" Signal Processing: Image Communication, 27(3): 249–259, 2012.

[19] Wei Z., Wu Y., Ding X., and Deng R. H., - A Scalable and Format Compliant Encryption Scheme for H. 264/SVC Bit Streams, Signal Processing: Image Communication, 27:1011–1024, 2012.

[20] Ghebleh M., Kanso A. and Noura H. -An Image Encryption Scheme Based on Irregularly Decimated Chaotic Maps, Signal Processing: Image Communication.

[21] Lima J. B., Lima E. A. O. and Madeiro F. - Image Encryption Based on the Finite Field Cosine Transform. Signal Processing: Image Communication, 28:1537–1547, 2013.

[22] Zhang Y., Xiao D., Shu Y., and Li J., "A Novel Image Encryption Scheme Based on a Linear Hyperbolic Chaotic System of Partial Differential Equations," Signal Processing: Image Communication, 28:292–300, 2013.

[23] Zhu H., Zhao C. and Zhang X., - A Novel Image Encryption Compression Scheme Using Hyper-chaos and Chinese Remainder Theorem, Signal Processing: Image Communication, 28:670–680, 2013.

[24] Fotopoulos V., Stavrinou M. L. and Skodras A. N.- Authentication and Self-Correction in Sequential MRI Slices," Journal of Digital Imaging, 24(5):943–948, 2011.

[25] Rahimi F. and Rabbani H. - A Dual Adaptive Watermarking Scheme in Contourlet Domain for DICOM Images, BioMedical Engineering Online, vol. 10, article 53, 2011.

[26] Elshazly E. H., Faragallah O. S., Abbas A. M., Ashour M. A., El-Rabaie E-S. M., Kazemian H., Alshebeii S. A., Fathi E., Hala A-E-S. and Elsayed H. S., - Robust and Secure Fractional Wavelet Image Watermarking. Signal, Image and Video Processing, 2014.

[27] Mousavi S. M., Naghsh A. and Abu-Bakar S. A. R., - Watermarking Techniques used in Medical Images: A Survey. Journal of Digital Imaging, 27(6):714-729, 2014.

[28] Rey C. and Dugelay J. L., (2002), " A Survey of Watermarking Algorithm for Image Authentication. EURASIP Journal on Applied Signal Processing, (1): 631-621, 2002.

[29] Allaert F. A. and Dusseire L. - Security of Health System in France: What We Do Will No Longer Be Different From What We Tell, International Journal of Biomedical Computing, 35(1):201-204, 1994.

[30] Delfs H. and Knebl H. - Introduction to Cryptography: Principles and Applications", Second Edition, Springer-Verlag Berlin Heidelberg, 2007.

[31] Stallings W. - "Cryptography and Network Security: Principles and Practice ", Seventh Edition, Pearson Education Limited, 2017.

[32] Biggs N. "Codes: An introduction to Information Communication and Cryptography" Springer, 2008.

[33] Mister S. and Tavares S. - Cryptanalysis of RC4-like Ciphers. In Tavares S. and Meijer H. eds.: Selected Areas of Cryptography (SAC '98). Volume 1556 of LNCS, SpringerVerlag 1999.

[34] Menezes A. J., van Oorschot P.C. and Vanstone S. A. - Handbook of Applied Cryptography. Chapter 6, pp 191-195, CRC Press, 1997.

[35] Fluhrer S., Mantin I. and Shamir A. - Weaknesses in the Key Scheduling Algorithm of RC4. In: Selected Areas of Cryptography (SAC 2001). LNCS, SpringerVerlag (2001)

[36] Cox I. J., Kilian J., Leighton F. T. and Shamoon T. - Secure Spread Spectrum Watermarking for Multimedia, Image Processing, IEEE Transactions 6(12): 1673-1687, 1997.

[37] Schyndel R. G., Tirkel A. and Osborne C. F. - A Digital Watermark , Proceedings of IEEE International conference on Image Processing, ICIP-1994, pp. 86-90, 1994.

[38] Zhang Y., Digital Watermarking Technology: A Review, ETP International Conference on Future Computer and Communication, IEEE, 2009.

[39] Pickholtz R., Schilling D. and Millstein L. - Theory of Spread Spectrum Communications: A Tutorial, IEEE Transactions on Communications, 30: 855-884, 1982

[40] Samcovic A. and Turan J. - Digital Image Watermarking by Spread Spectrum. In: Proceedings of the 11th WSEAS International Conference on Communications, Agios Nikolaos, Crete Island, Greece, July 26-28, 2007.

[41] Tolbal M. F., Ghonemy M. A.,. Taha I. A. and Khalifa A. S. - Using Integer Wavelet Transforms In colored Image-Steganography. International Journal of Intelligent Computing and Information Sciences, 4(2):1-11, 2004.

[42] Boucherkha S. and Benmohamed M. A. - Lossless Watermarking Based Authentication System for Medical Images, International Journal of Signal Processing, 1(4):278–81, 2004.

[43] Delforouzi A. and Pooyan M. - Adaptive Digital Audio Steganography Based on Integer Wavelet Transform. Circuits System Signal Process, 27:247–259, 2008.

[44] Memon N. and Gilani S., - Adaptive Data Hiding Scheme for Medical Images Using Integer Wavelet Transform". In: IEEE International Conference on Emerging Technologies, Islamabad, Pakistan; pp. 221–224, 2009.

[45] Luo, Z. Chen, M. Chen, X. Zeng and Z. Xiong - Reversible Image Watermarking Using Interpolation Techniques. IEEE Transactions on Information Forensics and Security, 5(1):187–193, 2010.

[46] Mostafa S., El- sheimy N., Tolba A., Abdelkader F. and Elhindy H., "Wavelet Packets-based Blind Watermarking for Medical Image Management", Open Biomedical Engineering Journal, 4: 93–98, 2010.

[47] Memon N. - Watermarking of Medical Images for Content Authentication and Copyright Protection", PhD thesis, Faculty of Computer Science and Engineering, GIK Institute of Engineering Sciences and Technology, Pakistan, 2010.

[48] Sakkara S., Akkamahadevi D. H. , Somashekar K. and Raghu K., - Integer Wavelet based Secret Data Hiding by Selecting Variable Bit Length. International Journal of Computer Applications 48(19): 7-11, 2012.

[49] Ko L., Chen J., Shieh Y., Hsin H. and Sung T. - Nested Quantization Index Modulation for Reversible Watermarking and its Application to Healthcare Information Management Systems. Computer Math Method Med 2012:1–8, 2012.

[50] Pandey V., Singh A. and Shrivastava M., - Medical Image Protection by Using Cryptography Data-Hiding and Steganography. International Journal of Emerging Technology and Advanced Engineering, 2(1):106-109, 2012.

[51] An L., Gao X., Xuelong L., Tao D., Deng C. and Li J. - Robust Reversible Watermarking via Clustering and Enhanced Pixel-wise Masking. IEEE Trans Image Process 21(8):3598–611, 2012.

[52] Das S. and Kundu M. - Effective Management of Medical Information through a Novel Blind Watermarking Technique. J Med Syst 36(5):3339–3351, 2012.

[53] Bouslimi D., Coatrieux G. and Roux C. - A Joint Encryption/Watermarking Algorithm for Verifying the Reliability of Medical Images: Application to Echographic Images". Comput Methods Programs, Biomed, 106(1):47–54, 2012

[54] Jain M., Choudhary R. C. and Kumar A. - Secure Medical Image Steganography with RSA Cryptography using Decision Tree. In: IEEE Second International Conference on Contemporary Computing and Informatics, 2016.

[55] Mahalakshmi V., Satheeshkumar S. and Sivakumar S. - Performance of Steganographic Methods In Medical Imaging, International Journal of Computational and Applied Mathematics, 12(1):549-556, 2017.

[56] Banjan N. and Dalvi P. - "Medical Data Security Using Combination of Cryptography and Steganography with AES-LSB Algorithm. International Journal of Advanced Research in Electronics and Communication Engineering, 7(7): 673-677, 2018.

[57] Abd-Eldayem, M. M. (2013). A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine. Egyptian Informatics Journal, 14(1), 1-13.

[58] Samcovic, A., & Turan, J. (2007, July). Digital image watermarking by spread spectrum. In *Proceedings of the 11th WSEAS International Conference on Communications* (pp. 26-28).