Secure Transmission and Recovery of Embedded Patient Information from Biomedical Images of Different Modalities through a Combination of Cryptography and Watermarking

Subhajit Koley[1]
[1]Electronics & Communication Engineering, Guru Nanak Institute of Technology, Kolkata, India
[1]subhajitgnitece@gmail.com

Koushik Pal[2], Goutam Ghosh[3]
[2,3]Institute of Radio Physics and Electronics, University of Calcutta, Kolkata, India
[2]koushik.rpe@gmail.com, [3]goggle.rpe@gmail.com

Mahua Bhattacharya[4]
[4]Indian Institute of Information, Technology and Management, Gwalior, India
[4]mahuabhatta@gmail.com

Abstract — In this paper a new type of information hiding skill in biomedical images is proposed through a combination of cryptography and digital watermarking to achieve the enhancement in confidential and authenticated data storage and secured transmission. Here patient's name and doctor's name are considered as patient's information which is encrypted using cryptography and embedded in the scan image of that patient through watermarking. RSA algorithm is used for encryption and higher order bit LSB replacement technique is used for embedding the information. The private keys are also embedded in the cover image to have better security and accurate recovery of the hidden information. The outcome of the proposed methodology shows that the hidden information doesn't affect the cover image and it can be recovered efficiently even from several noisy images. The strength of the proposed embedding scheme is also supported by several image quality matrices.

Index Terms — Biomedical image, Cryptography, Watermarking, LSB, ASCII, attacks, image quality metrics.

I. INTRODUCTION

Biomedical imaging is an important and vital aid in diagnostic and management decisions. In this regard, several different techniques are used: X-ray, Computer Tomography (CT) Scan, Magnetic Resonance Imaging (MRI), Positron Emission of Tomography (PET) etc. Critically ill or injured patients can be treated locally by effective and secured communication between remote hospitals and distant specialist and the issues the unified network protocols and different security settings in the data transfer arise [1-3]. The transmission of medical information among the geographically separated medical organizations is done in as secured way as possible [4-5]. In order to fulfill the security and convenience issues of the patients like the prevention of medical fault, the real-time detection of abnormal event, the support of clinical decision and development of medical service based on the patient, has to be achieved. Cryptography and watermarking is an important technology for these topics. In cryptography, the message is hidden in the form of cipher but an interception of the message can be damaging, as it still shows at the time of communication between the sender and receiver. In contrast, Watermarking takes a different approach in hiding the evidence. Watermarking embeds the message imperceptibly without changing image size or format. The appearance of the watermarking in order to contribute to the security of medical images shared on the network. We use both cryptography and watermarking technique for secure transmission of patient's information. If any unauthorized person recovers the watermark, still he can't get the original message. So, by this process we can achieve the enhancement in confidential and authenticated data storage and secured transmission.

A. Cryptography

Cryptography is the study of information hiding and verification. It includes the protocols, algorithms and strategies to securely and consistently prevent or delay unauthorized access to sensitive information and enable verifiability of every component in a communication. Cryptography concerns four main goals. They are: message confidentiality: Only an authorized recipient should be able to extract the contents of the message from its encrypted form, message integrity: The

recipient should be able to determine if the message has been altered, sender authentication: The recipient should be able to verify from the message, the identity of the sender, the origin or the path it travelled so to validate claims from emitter or to validated the recipient expectations, sender non-repudiation: The emitter should not be able to deny sending the message [6-7].

RSA Algorithm:

A popular algorithm in cryptography is RSA. RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm nowadays [8].

How the RSA System Works:

Key Generation Algorithm

Step 1: Generate two large random primes, p and q.
Step 2: Compute $n = p*q$ and $z = (p-1)(q-1)$.
Step 3: Choose a number relatively prime to z and call d.
Step 4: Find e such that $e*d = 1 \mod z$.
Step 5: The public key is (n, e) and the private key is (n, d).

Encryption

Sender A does the following:-
Step 1: Obtains the recipient B's public key (n, e).
Step 2: Represents the plaintext message as a positive integer m.
Step 3: Computes the ciphertext $c = m^e \mod n$.
Step 4: Sends the ciphertext c to B.

Decryption

Recipient B does the following:-
Step 1: Uses his private key (n, d) to compute $m = c^d \mod n$.
Step 2: Extracts the plaintext from the integer representative m.

B. Watermarking

Watermarking describes methods and technologies that hide information, like a number or text, in digital media, such as images, video or audio. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data. The hiding process has to be such that the modifications of the media are imperceptible. For images, this means that the modifications of the pixel values have to be invisible [9-11].

1. Classification of Digital Watermarking

1.1. According to the resistant ability of watermark
Watermarking technique can also be classified as robust and fragile [12].

Robust watermarking has the capability to resist various attacks or manipulations of the media.

Fragile watermarking, on the other hand, can be easily destroyed or remain irretrievable after modification is done on the image. Copyright protection is achieved by robust watermarking while image authentication is usually achieved by fragile schemes.

1.2. According to the visibility
Digital image watermarking may be classified as visible and invisible. The visible watermarks can be seen by normal eyes and can be visible on bills, television channel logos, currency notes, etc. Invisible watermarks are embedded secretly [13].

1.3. According to how watermark is detected and extracted Blind-extracting watermarking means watermark detection and extraction do not depend on the availability of original image. The drawback is when the watermarked image is seriously destroyed; watermark detection will become very difficult.

Non-blind - extracting watermark can only be detected by those who have a copy of original image. It guarantees better robustness but may lead to multiple claims of ownerships.

1.4. According to the domain for watermark
Watermarks can be applied in the spatial domain or in the transform (frequency) domain [14].

Spatial domain methods are based on direct modification of the values of the image pixels, so the watermark has to be imbedded in this way [15].

Frequency (transform) domain methods are based on the using of some invertible transformations like discrete cosine transform (DCT), discrete Fourier transform (DFT), discrete wavelet transform (DWT) etc. to the host image.

C. Biomedical image

The images which are used to diagnose and examine the disease in the human body are known as biomedical images. Biomedical images play a significant role in diagnosis of many diseases. Doctors diagnose from medical images, so more care is required to hide patient information in biomedical images without affecting quality of image [16]. During the diagnosis, it is important that an automated framework exists to verify the authenticity and integrity of the image itself. Biomedical images require special safety and confidentiality, because critical judgment is done on the information provided by biomedical images. Biomedical imaging is used to create biomedical images of the human body for clinical purpose or medical science including the study of normal anatomy and physiology [17].

2. Radiology Technology:

2.1. X-Ray Technology: The most common imaging technique used today is a radiograph (x-ray film) and the most common x-ray ordered is a chest x-ray, and the musculoskeletal x-ray exam comes in second. An x-ray provides a two dimensional image of the interior of the body and the procedure is performed by a Radiologic Technologist. A single x-ray passes through the body and exposes the film on a radiograph (or fluorescent screen) placed on the opposite side. Tissues having different densities show up as differing densities on the radiograph i.e. x-rays which have their nature of being absorbed to various degrees through body tissues depending on the density of them.

2.2. Computed Tomography (CT) Scan Technology: In CT Scanning x-rays moves in an arch around the part of the body being observed through a laser-like beam. The beams of x-rays passed through the region of the body imaged are collected by a special detector which converts the x-rays into electronic pulses that produce readings of the density of the tissue into a 1cm slice of the body. From these readings a computer can assemble a picture of the body called a CT Scan that can be viewed on a fluorescent screen, then photographed for later examinations. CT scan stands for computerized tomography. It obtains parts of the body that can't be seen on a standard x-ray with the help of computer algorithms in conjunction with the enhanced x-ray technology.

2.3. Magnetic Resonance Imaging (MRI) Technology: MRI uses the magnetic properties of the hydrogen nucleus, which is excited by radio frequency radiation transmitted by a coil surrounded by the body part. When placed in strong magnetic fields, the nuclei of certain atoms absorb radio frequencies beamed at them and then emit their own radio frequency waves. This process allows MRI Tech's and physicians to see very clear pictures of the inside of the body including tissues, organs, and blood vessels. MRI is a non-invasive technique that does not use ionizing radiation. MRI has become one of the primary tools used to image the brain, spinal cord, major blood vessels, and several key organs. The images can be produced in 3-D, which significantly enhances the physician's ability to diagnose problems. MRI Technicians are also used to help view the process of surgery in real time in 3-D, which assists with a whole host of surgical procedures.

D. Biomedical watermarking

Biomedical watermarking is a signal processing technique in order to achieve the objectives e.g. confidentiality, reliability, availability as well as traceability of medical information systems. Biomedical image watermarking is a relevant process for enhancing data security, content verification and image fidelity. Embedding external data in medical images should not change any information, thereby affecting further applications. Biomedical image watermarking embeds messages imperceptibly without changing image size or format. Protection of Electronic Patient Record (EPR) in digital health care system is very important. Hiding patient data as EPR in the medical image is one of the applications of digital image watermarking [18].

E. Description of Different Colour Spaces

Colour space is a system for describing colour numerically. It's also known as a 'colour model'. A colour model is an abstract mathematical model describing the way colours can be represented as tuples of numbers, typically as three or four values of colour components [19-20].

Gray Scale is an image in which the value of each pixel is a single sample, that is, it carries only intensity information. Images of this sort, also known as black-and-white, are composed exclusively of shades of gray,

varying from black at the weakest intensity to white at the strongest. Grayscale images have many shades of gray in between black and white. Grayscale images are often the result of measuring the intensity of light at each pixel in a single band of the electromagnetic spectrum and in such cases they are monochromatic proper when only a given frequency is captured. But also they can be synthesized from a full colour image. The intensity of a pixel is expressed within a given range between a minimum and a maximum, inclusive. This range is represented in an abstract way as a range from 0 (total absence, black) and 1 (total presence, white), with any fractional values in between. In the binary representations assume that 0 is black and the maximum value 255 is white.
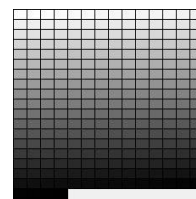

Figure 1. Gray-scale space

RGB is the simplest colour space. The RGB colour model is an additive colour model in which red, green, and blue light are added together in various ways to reproduce a broad array of colours. The name of the model comes from the initials of the three additive primary colours, red, green, and blue. The main purpose of the RGB colour model is for the sensing, representation, and display of images in electronic systems, such as televisions and computers, though it has also been used in conventional photography. Their wavelengths were standardized by the CIE in 1931: red=700 nm, green=546.1 nm and blue=435.8 nm.
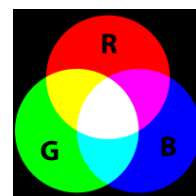

Figure 2. RGB colour space

YCbCr is a family of colour spaces commonly used to represent digital in video and digital photography systems. In this colour space, the Y denotes the luminance component. It means that Y shows the brightness that's luma. Chrominance information corresponds to the two colour-difference components Cb and Cr too. Cb is blue colour minus luma (B−Y) and Cr is red colour minus luma (R−Y). The transformation simplicity and explicit separation of luminance and chrominance components make this colour space attractive for skin colour modeling. When a still image in RGB form is being prepared for encoding under the JPEG image encoding and compression system, it is

transformed to the YCbCr colour space. In this colour space luminance (brightness) information is stored as a single component Y.
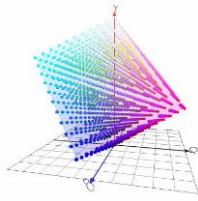

Figure 3. YCbCr colour space

Conversion from RGB to YCbCr:
The Matrix form:

$$\begin{pmatrix} Y \\ Cb \\ Cr \end{pmatrix} = \begin{pmatrix} 0.299 & 0.587 & 0.114 \\ -0.168636 & 0.232932 & -0.064296 \\ 0.499813 & -0.418531 & -0.081282 \end{pmatrix} \begin{pmatrix} R \\ G \\ B \end{pmatrix}$$

F. Attacks and distortions

In watermarking terminology, an "attack" is any processing that may impair detection of the watermark or communication of the information conveyed by the watermark. Broadly it can be classified as –Intentional Attacks and Non-Intentional Attacks. An attack may be performed intentionally on a watermarked document in order to destroy or degrade the quality of the hidden watermark. These distortions also introduce degradation on the performance of the watermark extraction algorithm. The success of a digital watermarking technology depends heavily on its robustness to withstand attacks that are aimed at removing or destroying the watermark from its host data. Some of the popular attacks mentioned in this paper are: (a) Salt and Pepper Noise, (b) Gaussian noise, (c) Image Compression, (d) Erosion, (e) Averaged noise, (f) Multiplicative noise, (g) Motion blur, (h) Dilation [21-24].

1) Salt and Pepper

Salt and Pepper Noise is a form of noise that replaces the intensity levels of some of the pixels of an image resulting in loss of information from those pixels. An image containing salt and pepper noise represents itself as randomly occurring dark pixels in bright regions and bright pixels in dark regions. This type of noise can be caused by analog-to-digital converter errors, bit errors in transmission, etc.

2) Image Compression

To reduce the size, high quality images like BMP images are converted to JPEG. Compression is a common form of attack, as data transferred via a network is often compressed using JPEG. The degree of compression can be adjusted.

3) Gaussian noise

Gaussian noise is statistical in nature that has its probability density function equal to that of the normal distribution. It can degrade the watermark image quality and may destroy the watermark.

4) Erosion

Erosion removes pixels on object boundaries. The number of pixels added or removed from the objects in an image depends on the size and shape of the structuring element used to process the image.

5) Averaged

The former describes an attack in which many instances of a given data set, each time signed with a different key or different watermark, are averaged to compute the attacked data.

6) Multiplicative noise

Multiplicative noise, also known as speckle noise, is a signal dependent form of noise whose magnitude is related to the value of the original pixel. This noise can also degrade the quality of the watermark image by manipulating the hidden information or watermark.

7) Motion Blur

Motion blurs the artifact by which fast-moving objects appear blurred. Each frame in a conventional film is an average sample taken over about half the time it takes to record the frame. In consequence, fast-moving images appear blurred. Temporal aliasing is more severe in the case of computer-generated images where the image is likely to be defined at a specific point in time. In computer animation, the created images are often deliberately blurred to achieve a similar effect to the conventional camera and enhance the simulation of motion.

8) Dilation

Dilation is another basic operation in morphological image processing. Originally developed for binary images, it has been expanded first to grayscale images, and then to complete lattices. The dilation operation usually uses a structuring element for probing and expanding the shapes contained in the input image. Dilation is the dual operation of the erosion. Figures that are very lightly drawn get thicker when "dilated".

G. Image quality metrics

Image quality metrics measures the perceived image degradation, compared to an ideal or perfect image. Imaging systems may introduce some amounts of distortion in the signal, so the quality assessment is an important problem. Measurement of the quality of watermarked image and attacked watermarked image is very important for the watermarking technique to prove its strength and successfulness. To measure the amount of visual quality degradation between the original and watermarked images different types of image quality metrics such as PSNR, SSIM, BER, SC, NCC, and UIQI are used [25-26].

A higher Peak signal -to-noise ratio (PSNR) would normally indicate that the reconstruction is of higher quality. A small value of PSNR indicates poor quality. Structural Similarity Index Measure (SSIM) is a method for measuring the similarity between two images. Structural Content (SC) is the measure of information content in the image. The Bit Error Rate (BER) can be considered as an approximate estimate of the bit error probability. This estimate is accurate for a long time interval and a high number of bit errors [27-29].

II. PROPOSED METHODOLOGY

A. *Embedding algorithm*

A biomedical gray-scale or colour image is taken as cover image which is divided into four parts: upper left, upper right, lower left, lower right to hide different information. Then upper left part and lower right part are taken and the RGB is converted into YCbCr colour space and colour components Y, Cb, Cr are extracted from YCbCr colour space image. The patient's name and the doctor's name are taken as a patient's record and it is converted into its ASCII value and it is flipped. The flipped ASCII values or plain texts are then converted into the cipher text using RSA algorithm encryption method with the help of private key and public key. 2 sets of prime no's are taken to generate public keys and private keys. The cipher text is converted into its 8 bit binary digit and thus the watermark is generated. After that the watermark is embedded into some pixels of Cb, Cr components using replacing slightly higher order bit LSB. The upper right and lower left part of the cover image is taken and the YCbCr is converted to RGB colour space and extracted colour components Y, Cb, Cr. Keys are embedded into Cb, Cr components of cover image using LSB replacement method. Once the data has been embedded, the 4 parts of the image are joined and converted into RGB to YCbCr colour space and hence the watermarked image is created. Flowchart of the embedding technique is given in Figure.4.

B. *Recovery algorithm*

The watermarked image is taken and it is divided into four parts: upper left, upper right, lower left, lower right. The upper right part and lower left part of the watermarked image is taken and the RGB is converted into YCbCr colour space. The colour components Y, Cb, Cr are extracted from YCbCr colour space image. The watermark values are decoded from higher order bit LSB of the watermarked image by LSB flipping method to recover the hidden keys which helps to decrypt hidden the encrypted patient's and doctor's name. The patient's information is recovered from upper left and lower right part of the watermarked image. Using two sets of keys given by the users, the public keys and the private keys are generated. After that the watermark or the cipher text is converted into plain text using RSA algorithm decryption method with the help of above mentions keys. The plain texts are then flipped. The obtained binary streams are converted into ASCII values and then its equivalent alphanumeric values. Thus the encrypted hidden patient's record i.e. the patient's name and doctor's names are recovered. Once the data has been decoded, the 4 parts of the image are joined together. Thus, we recover the original biomedical image and also various hidden information. Flowchart of the recovery technique is given in Figure.5.

III. RESULT AND DISCUSSION

In this section the outcome of the proposed methodology is depicted along with some important image quality metrics to describe the quality of both the embedding and detection algorithm. In Table 1 and Table 3, nine sets of gray-scale biomedical images and nine sets of colour biomedical images of different modalities like X- Ray, CT Scan, MRI along with patient information and obtained watermarked images are given. Primarily we have considered the communication is ideal and hence no external interference has been included. The calculated value of the quality metrics such as PSNR and SSIM, SC, NCC, BER, UIQI are also given to find the image quality degradation. It is observed that the difference between the watermarked image and the cover image by the Human Visual System appear to be identical. From Table 1 and Table 3, we observe that the PSNR value is quite higher which indicates good quality of picture. The value of SSIM in all the cases is close to 1 which describes a good structural similarity between the original and watermarked image and BER is close to 0 which indicates less error in watermarked image. The value of NCC and UIQI are also close to 1 which is proof of the good quality of the watermarked image. We can also see that patient information is successfully recovered from the watermarked images which are exactly same as the hidden one.

Further values of different image quality metrics also state that the proposed methodology is successfully applicable for both gray scale and colour biomedical images of different modalities. The values of image quality metrics for gray scale X-Ray and CT Scan is better while it is better in case of colour CT Scan biomedical images.

In practice in the real world scenario there are chances of unauthorized users in reality where the watermarked image can also be easily altered by unauthorized access from unwanted users. Different types of attacks such as salt and pepper noise, image compression, gaussian noise, erosion, averaged, motion blur, multiplicative, dilated are applied on watermarked image and it is shown in Table 2 and Table 4. The values of PSNR and SSIM are lowered and BER is increased for different type of attacks. Moreover, from the experimental results it is clearly observed that the proposed technique can resist different types of moderately higher order attacks and still can recover the exact hidden information.
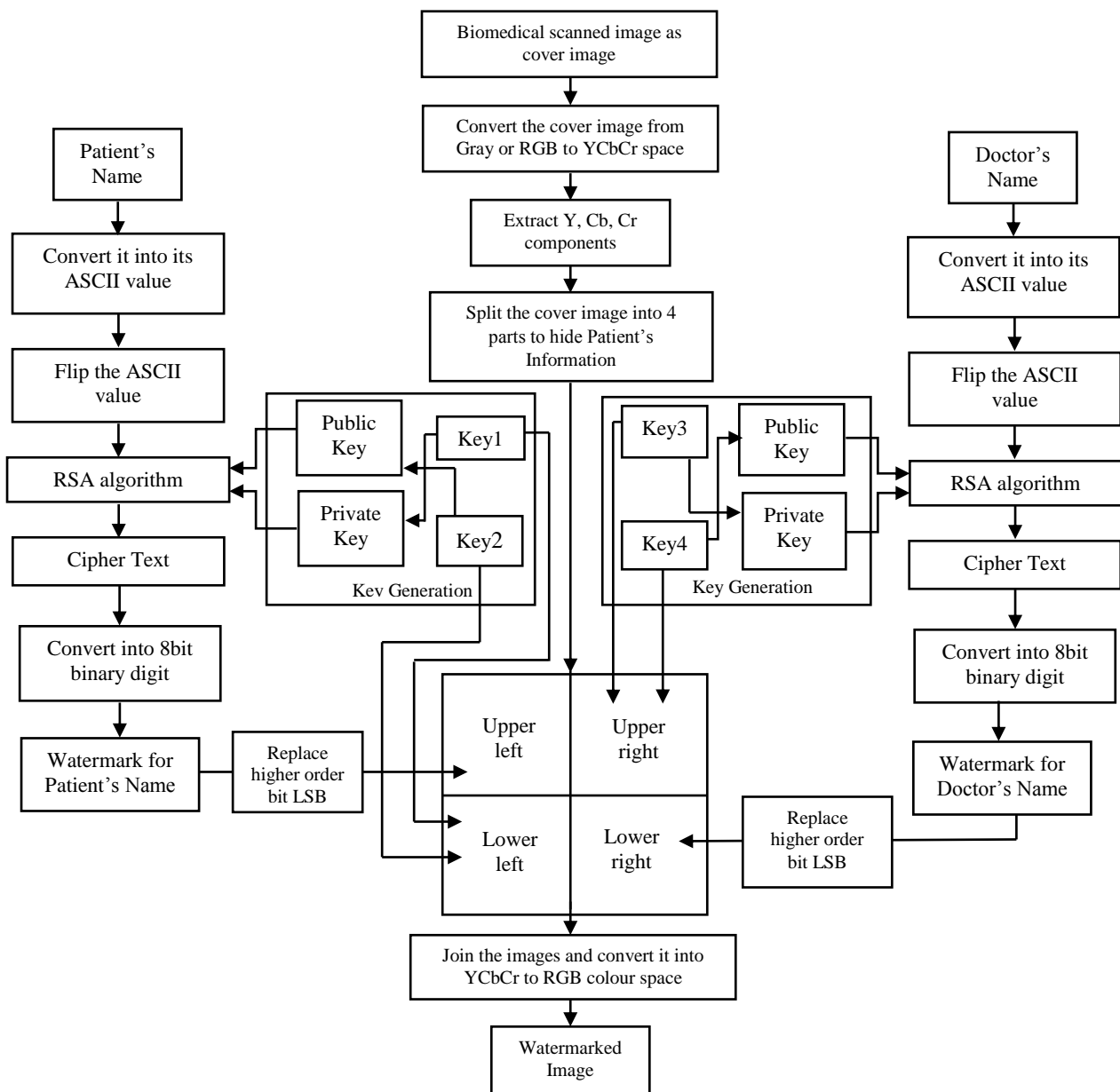
Secure Transmission and Recovery of Embedded Patient Information from Biomedical Images of
Different Modalities through a Combination of Cryptography and Watermarking

23
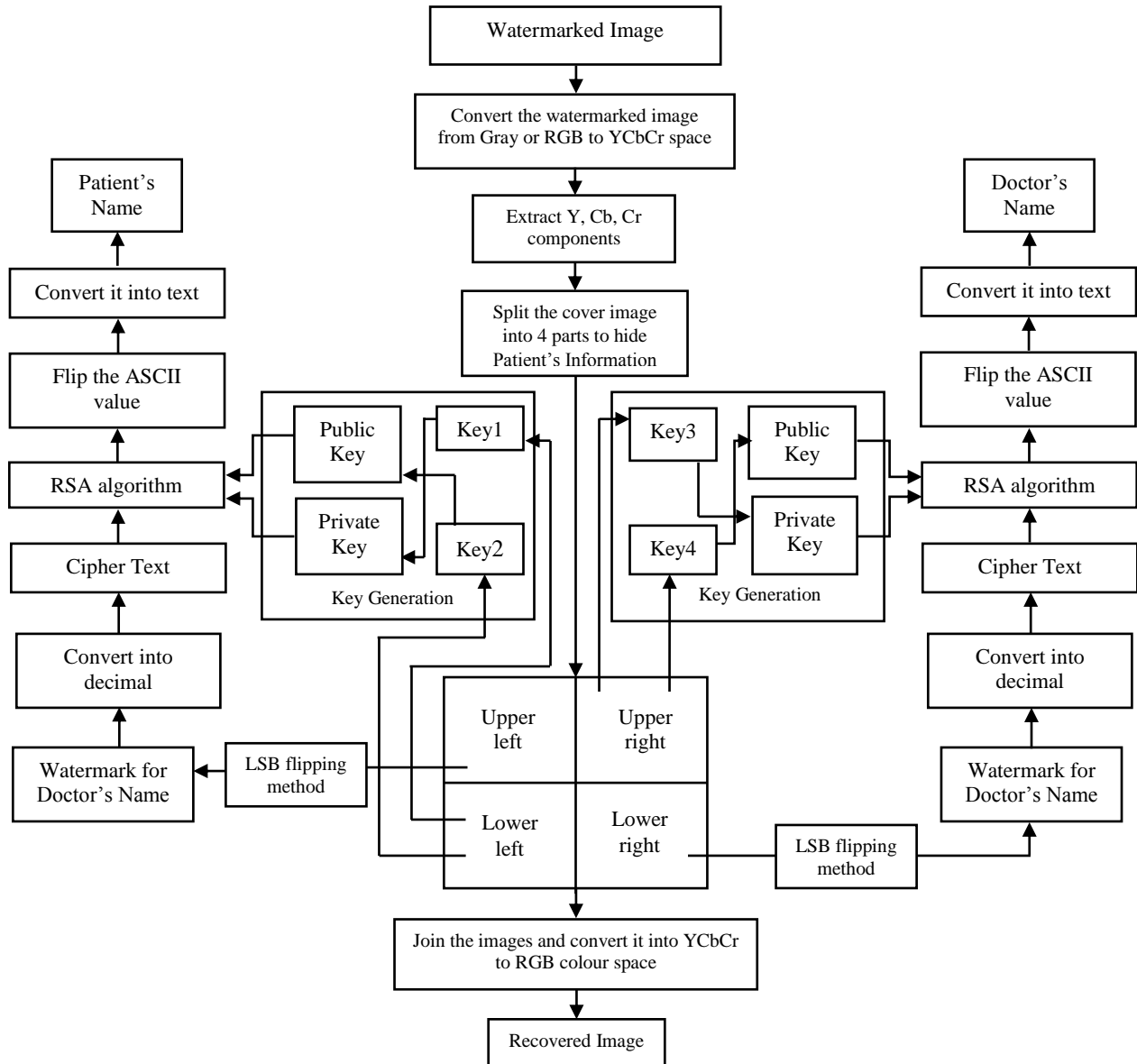
Figure 4. Flowchart of the proposed embedding technique

Figure 5. Flowchart of the proposed recovery technique

VI. CONCUSION

The biomedical image watermarking has the potential to provide complementary and alternative solutions in a range of issues of critical importance to health informatics, data authentication, and efficient medical data management, storage, and retrieval as well. The proposed combined cryptography and watermarking scheme addresses the above issues by imperceptibly embedding encrypted patient's information using RSA algorithm into the higher order bit LSB of the biomedical images. The experimental results describe that the proposed algorithm is robust against different type of attacks which also utilizes some a private keys which is required for the recovery of the hidden information and hence lending security to the algorithm. The obtained values of different image quality metrics support the quality of the encryption method visually and statistically. The exact recovery of the patient information from both the un-attacked and attacked watermarked image describes the strength of the recovery process. Hence we can conclude by stating the fact that the proposed methodology which is a combination of cryptography and watermarking provides a new method for authenticated information hiding and secure transmission that could be extended and integrated into healthcare information systems, in order to provide an additional level of security for accurate diagnosis and best practice treatment.

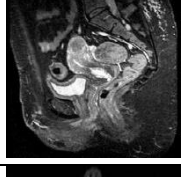TABLE I. EXPERIMENTAL RESULTS FOR GRAY-SCALE BIOMEDICAL IMAGES AND IMAGE QUALITY METRICS
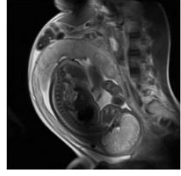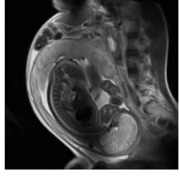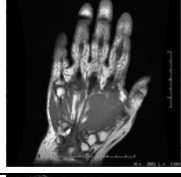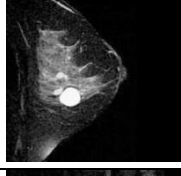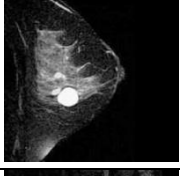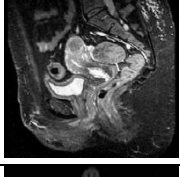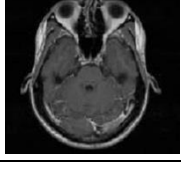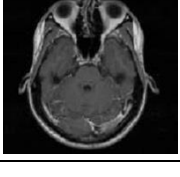
Cover Image	Data to be Hidden		Watermarked Image	Image Quality Metrics		Recovered Data	
	Patient's Record					Patient's Record	
Woman's Chest X-Ray	Patient's Name	Partho Bag		PSNR	56.047	Patient's Name	Partho Bag
				BER	0.161		
				SC	0.999		
	Doctor's Name	Dr. Sachin Gupta		SSIM	0.996	Doctor's Name	Dr. Sachin Gupta
				NCC	1		
				UIQI	0.938		
Ankle MRI	Patient's Name	Tamajit Nag		PSNR	55.176	Patient's Name	Tamajit Nag
				BER	0.197		
				SC	0.999		
	Doctor's Name	Dr. Yuvraja T.B		SSIM	0.998	Doctor's Name	Dr. Yuvraja T.B
				NCC	1		
				UIQI	0.997		
Womb MRI	Patient's Name	Shrotriya Sarkar		PSNR	55.833	Patient's Name	Shrotriya Sarkar
				BER	0.169		
				SC	0.998		
	Doctor's Name	Dr. Ravi K Arora		SSIM	0.998	Doctor's Name	Dr. Ravi K Arora
				NCC	1		
				UIQI	0.959		
Dental Cavity X-Ray	Patient's Name	Rahul Chakraborty		PSNR	56.167	Patient's Name	Rahul Chakraborty
				BER	0.157		
				SC	0.998		
	Doctor's Name	Dr. A K Jotwani		SSIM	0.999	Doctor's Name	Dr. A K Jotwani
				NCC	1		
				UIQI	0.998		
Abdomen CT Scan	Patient's Name	Kaustabh Ghatak		PSNR	57.654	Patient's Name	Kaustabh Ghatak
				BER	0.111		
				SC	0.998		
	Doctor's Name	Dr. P V Reddy		SSIM	0.999	Doctor's Name	Dr. P V Reddy
				NCC	1		
				UIQI	0.997		
Hand MRI	Patient's Name	Avijit Sarkar		PSNR	55.811	Patient's Name	Avijit Sarkar
				BER	0.17		
				SC	0.998		
	Doctor's Name	Dr. Santanu Sen		SSIM	0.995	Doctor's Name	Dr. Santanu Sen
				NCC	1		
				UIQI	0.914		
Breast X-Ray	Patient's Name	Sunita Dhar		PSNR	53.883	Patient's Name	Sunita Dhar
				BER	0.265		
				SC	0.998		
	Doctor's Name	Dr. Indira Ghosh		SSIM	0.983	Doctor's Name	Dr. Indira Ghosh
				NCC	1		
				UIQI	0.726		
Pelvis Gynae MRI	Patient's Name	Sweta Das		PSNR	56.07	Patient's Name	Sweta Das
				BER	0.16		
				SC	0.998		
	Doctor's Name	Dr Nirmala Dey		SSIM	0.999	Doctor's Name	Dr Nirmala Dey
				NCC	1		
				UIQI	0.995		
Brain CT Scan	Patient's Name	Jayanta Dhara		PSNR	54.459	Patient's Name	Jayanta Dhara
				BER	0.232		
				SC	0.997		
	Doctor's Name	Dr. Bapi Singh		SSIM	0.995	Doctor's Name	Dr. Bapi Singh
				NCC	1		
				UIQI	0.867		

TABLE II. EXPERIMENTAL RESULTS WITH ATTACK FOR GRAY-SCALE BIOMEDICAL IMAGES AND IMAGE QUALITY METRICS
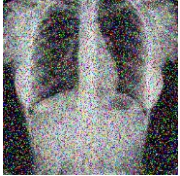
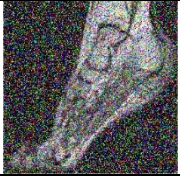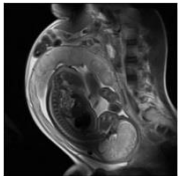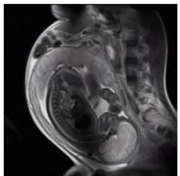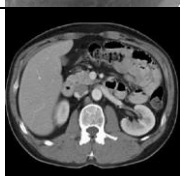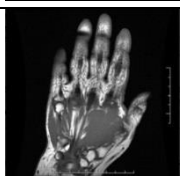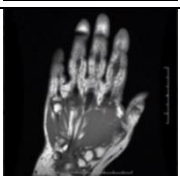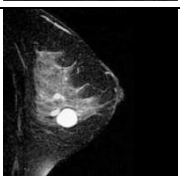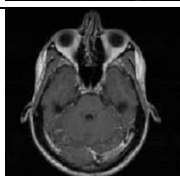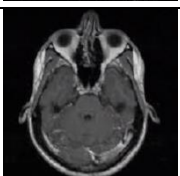| Watermarked Image		Data to be Hidden Patient's Record		Attacked Image		Image Quality Metrics		Recovered Data Patient's Record	
Woman's chest X-Ray		Patient's Name	Partho Bag	30% Salt & Paper		PSNR	12.932	Patient's Name	Partho Bag
						BER	0.657		
						SC	0.964		
		Doctor's Name	Dr. Sachin Gupta			SSIM	0.097	Doctor's Name	Dr. Sachin Gupta
						NCC	0.931		
						UIQI	0.115		
Ankle MRI		Patient's Name	Tamajit Nag	40% Salt & Paper		PSNR	10.717	Patient's Name	Tamajit Nag
						BER	0.719		
						SC	0.691		
		Doctor's Name	Dr. Yuvraja T.B			SSIM	0.109	Doctor's Name	Dr. Yuvraja T.B
						NCC	0.934		
						UIQI	0.133		
Womb MRI		Patient's Name	Shrotriya Sarkar	9% JPEG Compressed		PSNR	40.538	Patient's Name	Shrotriya Sarkar
						BER	0.801		
						SC	0.997		
		Doctor's Name	Dr. Ravi K Arora			SSIM	0.976	Doctor's Name	Dr. Ravi K Arora
						NCC	1.000		
						UIQI	0.966		
Dental Cavity X-Ray		Patient's Name	Rahul Chakraborty	Erode		PSNR	24.484	Patient's Name	Rahul Chakraborty
						BER	0.471		
						SC	1.165		
		Doctor's Name	Dr. A K Jotwani			SSIM	0.775	Doctor's Name	Dr. A K Jotwani
						NCC	0.913		
						UIQI	0.649		
Abdomen CT Scan		Patient's Name	Kaustabh Ghatak	Gaussian		PSNR	51.106	Patient's Name	Kaustabh Ghatak
						BER	0.445		
						SC	0.996		
		Doctor's Name	Dr. P V Reddy			SSIM	0.996	Doctor's Name	Dr. P V Reddy
						NCC	1.001		
						UIQI	0.933		
Hand MRI		Patient's Name	Avijit Sarkar	Averaged		PSNR	30.971	Patient's Name	Avijit Sarkar
						BER	0.639		
						SC	1.034		
		Doctor's Name	Dr. Santanu Sen			SSIM	0.952	Doctor's Name	Dr. Santanu Sen
						NCC	0.978		
						UIQI	0.77		
Breast X-Ray		Patient's Name	Sunita Dhar	Multiplicative		PSNR	64.029	Patient's Name	Sunita Dhar
						BER	0.025		
						SC	1		
		Doctor's Name	Dr. Indira Ghosh			SSIM	0.999	Doctor's Name	Dr. Indira Ghosh
						NCC	0.999		
						UIQI	0.999		
Pelvis Gynae MRI		Patient's Name	Sweta Das	Motion Blur		PSNR	30.723	Patient's Name	Sweta Das
						BER	0.857		
						SC	1.029		
		Doctor's Name	Dr Nirmala Dey			SSIM	0.922	Doctor's Name	Dr Nirmala Dey
						NCC	0.981		
						UIQI	0.907		
Brain CT Scan		Patient's Name	Jayanta Dhara	Dilated		PSNR	28.354	Patient's Name	Jayanta Dhara
						BER	0.525		
						SC	0.874		
		Doctor's Name	Dr. Bapi Singh			SSIM	0.923	Doctor's Name	Dr. Bapi Singh
						NCC	1.058		
						UIQI	0.715		

TABLE III. EXPERIMENTAL RESULTS FOR COLOUR BIOMEDICAL IMAGES AND IMAGE QUALITY METRICS
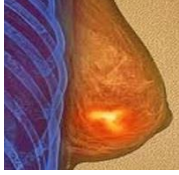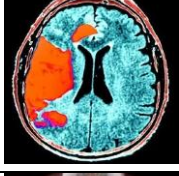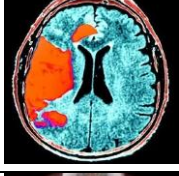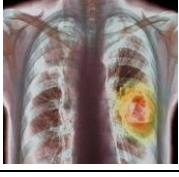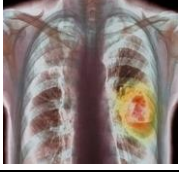
Cover Image	Data to be Hidden Patient's Record		Watermarked Image	Image Quality Metrics		Recovered Data Patient's Record	
Knee Joint CT Scan	Patient's Name	Sahanur Jaman		PSNR	54.836	Patient's Name	Sahanur Jaman
				BER	0.212		
				SC	1		
	Doctor's Name	Dr. Debashis Dutta		SSIM	0.999	Doctor's Name	Dr. Debashis Dutta
				NCC	0.999		
				UIQI	0.975		
Uterine MRI	Patient's Name	Sonali Bhowmik		PSNR	54.836	Patient's Name	Sonali Bhowmik
				BER	0.212		
				SC	1		
	Doctor's Name	Dr. Mamata Dutta		SSIM	0.999	Doctor's Name	Dr. Mamata Dutta
				NCC	0.999		
				UIQI	0.975		
Lumbar MRI	Patient's Name	Suparna Roy		PSNR	54.782	Patient's Name	Suparna Roy
				BER	0.216		
				SC	1		
	Doctor's Name	Dr. Jaydev Sengupta		SSIM	0.999	Doctor's Name	Dr. Jaydev Sengupta
				NCC	0.999		
				UIQI	0.991		
Lung CT Scan	Patient's Name	Rahul Chakraborty		PSNR	55.202	Patient's Name	Rahul Chakraborty
				BER	0.196		
				SC	1		
	Doctor's Name	Dr. Gopal Gulgulia		SSIM	0.999	Doctor's Name	Dr. Gopal Gulgulia
				NCC	0.999		
				UIQI	0.995		
Mammogram MRI	Patient's Name	Sebanti Sammadar		PSNR	54.861	Patient's Name	Sebanti Sammadar
				BER	0.212		
				SC	1		
	Doctor's Name	Dr. Indira Ghosh		SSIM	0.999	Doctor's Name	Dr. Indira Ghosh
				NCC	0.999		
				UIQI	0.998		
Leg MRI	Patient's Name	Gourav Ghosh		PSNR	54.72	Patient's Name	Gourav Ghosh
				BER	0.218		
				SC	1		
	Doctor's Name	Dr. Rajib Pyne		SSIM	0.998	Doctor's Name	Dr. Rajib Pyne
				NCC	0.999		
				UIQI	0.995		
Foetus MRI	Patient's Name	Poonam Ghosh		PSNR	54.72	Patient's Name	Poonam Ghosh
				BER	0.218		
				SC	1		
	Doctor's Name	Dr. Debjani Mukherjee		SSIM	0.998	Doctor's Name	Dr. Debjani Mukherjee
				NCC	0.999		
				UIQI	0.995		
Brain CT Scan	Patient's Name	Pinaki Saha		PSNR	54.497	Patient's Name	Pinaki Saha
				BER	0.23		
				SC	1		
	Doctor's Name	Dr. U D Gupta		SSIM	0.994	Doctor's Name	Dr. U D Gupta
				NCC	0.999		
				UIQI	0.891		
Chest X-Ray	Patient's Name	Arnab Sinha		PSNR	54.813	Patient's Name	Arnab Sinha
				BER	0.214		
				SC	1		
	Doctor's Name	Dr. Dhiman Sen		SSIM	0.999	Doctor's Name	Dr. Dhiman Sen
				NCC	0.999		
				UIQI	0.999		

TABLE IV. EXPERIMENTAL RESULT WITH ATTACK FOR COLOUR BIOMEDICAL IMAGES AND IMAGE QUALITY METRICS

Watermarked Image	Data to be Hidden Patient's Record		Attacked Image	Image Quality Metrics		Recovered Data Patient's Record	
Knee Joint CT Scan	Patient's Name	Sahanur Jaman	10% Salt & Paper	PSNR	17.711	Patient's Name	Sahanur Jaman
				BER	0.243		
				SC	0.950		
	Doctor's Name	Dr. Debashis Dutta		SSIM	0.384	Doctor's Name	Dr. Debashis Dutta
				NCC	0.985		
				UIQI	0.404		
Uterine MRI	Patient's Name	Sonali Bhowmik	20% Salt & Paper	PSNR	14.95	Patient's Name	Sonali Bhowmik
				BER	0.473		
				SC	1.005		
	Doctor's Name	Dr. Mamata Dutta		SSIM	0.333	Doctor's Name	Dr. Mamata Dutta
				NCC	0.948		
				UIQI	0.366		
Lumbar MRI	Patient's Name	Suparna Roy	30% Salt & Paper	PSNR	12.733	Patient's Name	Suparna Roy
				BER	0.624		
				SC	1.039		
	Doctor's Name	Dr. Jaydev Sengupta		SSIM	0.185	Doctor's Name	Dr. Jaydev Sengupta
				NCC	0.894		
				UIQI	0.225		
Lung CT Scan	Patient's Name	Rahul Chakraborty	Multiplicative	PSNR	56.570	Patient's Name	Rahul Chakraborty
				BER	0.143		
				SC	0.999		
	Doctor's Name	Dr. Gopal Gulgulia		SSIM	0.999	Doctor's Name	Dr. Gopal Gulgulia
				NCC	1		
				UIQI	0.999		
Mammogram MRI	Patient's Name	Sebanti Sammadar	Motion Blur	PSNR	37.713	Patient's Name	Sebanti Sammadar
				BER	0.717		
				SC	1.003		
	Doctor's Name	Dr. Indira Ghosh		SSIM	0.98	Doctor's Name	Dr. Indira Ghosh
				NCC	0.997		
				UIQI	0.972		
Leg MRI	Patient's Name	Gourav Ghosh	Gaussian	PSNR	50.826	Patient's Name	Gourav Ghosh
				BER	0.458		
				SC	0.997		
	Doctor's Name	Dr. Rajib Pyne		SSIM	0.997	Doctor's Name	Dr. Rajib Pyne
				NCC	1.001		
				UIQI	0.99		
Foetus MRI	Patient's Name	Poonam Ghosh	Erode	PSNR	17.95	Patient's Name	Poonam Ghosh
				BER	0.552		
				SC	1.225		
	Doctor's Name	Dr. Debjani Mukherjee		SSIM	0.63	Doctor's Name	Dr. Debjani Mukherjee
				NCC	0.888		
				UIQI	0.635		
Brain CT Scan	Patient's Name	Pinaki Saha	Dilated	PSNR	22.379	Patient's Name	Pinaki Saha
				BER	0.417		
				SC	0.898		
	Doctor's Name	Dr. U D Gupta		SSIM	0.879	Doctor's Name	Dr. U D Gupta
				NCC	1.042		
				UIQI	0.814		
Chest X-Ray	Patient's Name	Arnab Sinha	Erode	PSNR	19.994	Patient's Name	Arnab Sinha
				BER	0.525		
				SC	1.166		
	Doctor's Name	Dr. Dhiman Sen		SSIM	0.684	Doctor's Name	Dr. Dhiman Sen
				NCC	0.915		
				UIQI	0.675		

REFERENCES

[1] Rajendra Acharya U., P. Subbanna Bhat, Sathish Kumar, Lim Choo Min, "Transmission and storage of medical images with patient information, Computers in Biology and Medicine" 33, pg. 303–310, 2003.

[2] F. Cao, H. K. Huang, X. Q. Zhou, "Medical image security in a HIPAA mandated PACS environment". Computerized Medical Imaging and Graphics, 27 (2-3), pg. 185-196, 2003.

[3] Jasni Zain and Malcolm Clarke, "Security In Telemedicine: Issues In Watermarking Medical Images," Sciences of Electronic, Technologies of Information and Telecommunications, Tunisia, 2005.

[4] R. Ibrahim, T. S. Kuan, Steganography Imaging (SIS): "Hiding Secret Message inside an Image". Proceedings of the World Congress on Engineering and Computer Science, San Francisco, USA. 2010.

[5] Nayak, P Subbanna Bhat, R. Acharya and Niranjan; "Simultaneous storage of medical images in the spatial and frequency domain: a comparative study"; BioMedical Engineering OnLine , pp:3-17,2004.

[6] G N Swamy, K Srinivasa Rao, A Ravi Kumar; "A watermarking technique based on visual cryptography"; Journal of Information Assurance and Security 4, pp:470-473,2009.

[7] J. Dittmann, P. Wohlmacher, Klara Nahrstedt; "Multimedia and security using cryptographic and watermarking algorithm" ieee multimedia © IEEE, 2001.

[8] Behrouz A. Forouzan, Data Communications and Networking, 4/e, McGraw-Hill Higher Education, ISBN: 0072967757, 2007.

[9] G. Langelaar, I. Setyawan, R. Lagendijk, Watermarking digital image & video data. IEEE Signal Processing Magazine, pg. 20-46, 2000.

[10] A. Tirkel, G. Rankin, R. V. Schyndel, H. Mee, N. Osborne, Electronic watermark. In Proceedings of DICTA. pg. 666–672, 1993.

[11] A. K. Jain, "Fundamentals of Digital Image Processing", Prentice–Hall, Englewood Cliffs, NJ.

[12] I. J. Cox, M. Miller, J. Bloom, "Digital Watermarking," Morgan Kaufmann Publishers, 2002.

[13] W. K. Pratt, Digital Image Processing 4th Edition, John Wiley & Sons, Inc., Los Altos, California, 2007.

[14] R. C. Gonzalez and R.E. Woods, Digital Image Processing 2nd Edition, Prentice Hall, New Jersey, 2002.

[15] B. Smithal and K.A. Navas, "Spatial Domain-High Capacity Data Hiding in ROI Images", IEEE - ICSCN 2007.

[16] E. Koch, J. Rindfrey, J. Zhao, Copyright protection for multimedia data. In Proceeding sof the Int. Conf. on Digital Media and Electronic Publishing, 1994.

[17] T. Lehmann, A. Sovakar, W. Schmitt, R. Repges, "A comparison of similarity measures for digital subtraction radiography". Comput. Biol. Med. 27, pg. 151–167, 1997.

[18] H. M. Chao, C. M. Hsu, and S. G. Miaou, "A data-hiding technique with authentication, integration, and confidentiality for electronic patients records," in the IEEE Transactions Information Technology in Biomedicine, pp. 46-53, 2002.

[19] S. Walton, "Information authentication for a slipppery new age", Dr. Dobbs Journal, vol. 20, no. 4, pp.18-26, 1995.

[20] Yang,Y. and Bao, F., "An Invertible Watermarking Schemes for Authentication of Electronic Clinical Brain Atlas", ICASSP, 2003.

[21] K. Pal, G. Ghosh, M. Bhattacharya, "A Novel Digital image Watermarking Scheme for Data Security using Bit Replacement and Majority Algorithm Technique", Watermarking, Vol 1, ISBN- 979-953-307-583-8, INTECH Publication, Croatia, Europe, pp-117-132, 2012.

[22] A. Umaamaheshvari, K. Thanushkodi; "high performance and effective watermarking scheme for medical images"; European Journal of Scientific Research,ISSN 1450-216X Vol.67 No.2, pp:283-293, 2012.

[23] C. Song, S. Sudiman, M. Merabti, "A Spatial and Frequency Domain Analysis of the Effect of Removal Attacks on Digital Image Watermarks" ISBN: 978-1-902560-24-3, PGNet, 2012.

[24] J.Samuel Manoharan, Dr.Kezi C.Vijila, A.Sathesh, "Performance Analysis of Spatial and Frequency Domain Multiple Data Embedding Techniques towards Geometric Attacks", International Journal of Security (IJS), Volume (4) : Issue (3) pp. 28-37.

[25] K. Pal, G. Ghosh, M. Bhattacharya, "Retrieval of Hidden Infected Region using Biomedical Image Watermarking for Tele-diagnosis to Ensure Better Treatment", IEEE International Conference on Computers & Devices for Communication, Kolkata, 17-19 December 2012.

[26] K. Pal, G. Ghosh, M. Bhattacharya, "Reversible Digital Image Watermarking using Bit Replacement and Majority Algorithm Technique", Journal of Intelligent Learning Systems and Applications, ISSN: 2150-8402, Scientific Research Incorporation group, USA, Vol 4, Number-3, pp.199-206, August 2012.

[27] M. Eskicioglu and P. S. Fisher, "Image Quality Measures and Their Performance," IEEE Transactions on Communications, vol. 43, no. 12, pp. 2959-2965, December 1995.

[28] S. Koley, K. Pal, G. Ghosh, M. Bhattacharya, "Extraction and Authentication of Hidden Patient's Information from Biomedical Image through Crypto-Watermarking Technique", ISBN: 978-81-923777-9-7, pp. 183-188, 2013.

[29] K. Pal, G. Ghosh, M. Bhattacharya, "Biomedical Watermarking: An Emerging and Secure Tool for Data Security and Better Tele-d

iagnosis in Modern Health Care System"- in "Research Development in Computer Vision and Image Processing: Methodologies and Applications", ISBN: 9781466645585, IGI Global, Pennsylvania, USA, pp-208-234, DOI:10.4018/978-1-4666-4558-5.ch012, Aug, 2013.

AUTHORS

Subhajit Koley was born in Kolkata, India in 1991. He received the B. Tech. degree from West Bengal University of Technology (WBUT), in 2013. He has published over 10 refereed journal and National & International conference papers in the areas of Cryptography, Image Processing and Signal Processing. His representative published articles list as follow: A New Combined Crypto-Watermarking Technique using RSA Algorithm and Discrete Cosine Transform to Retrieve Embedded EPR from Noisy Bio-Medical Images (IEEE CATCON 2013, India), Extraction and Authentication of Hidden Patient's Information from Biomedical Image through Crypto-Watermarking Technique (IEMCON 2013, India), etc. Moreover, he was a participant of a straight light project for Micro, Small and Medium Enterprises. His activities currently focus on GUI based Breast Cancer Identification and Diagnostic System for Mammographic Image. His research interests include Security Aspects of Biomedical Image Watermarking, Cryptography, Digital Image Processing, Digital Signal Processing and Analog and Digital Communication and Electronic Devices;

Koushik Pal was born on 23rd February, 1983. He completed his B. Tech in Electronics and Communication Engineering from Vidyasagar University in 2004 and M. Tech in Radio Physics and Electronics from the Institute of Radio Physics and Electronics, University of Calcutta in 2007. He is presently pursuing his Ph. D. (Tech.) in Radio Physics and Electronics of the University of Calcutta. He joined the Department of Electronics and Communication Engineering as an Assistant Professor at Guru Nanak Institute of Technology, Kolkata in 2007. He is also associated with West Bengal University of Technology and Ramakrishna Mission Vivekananda Centenary College as a guest faculty. His research interests are in the fields of Security Aspects of Biomedical Image Watermarking, Digital Image Processing, Digital Signal Processing and Analog and Digital Communication. He has to his credit eight international journal publications and two

international book chapters and around twenty international and national conference publications;

Goutam Ghosh was born in 1949. He graduated with Physics Honours in 1969 from the University of Calcutta and thereafter obtained the B.Tech. degree in Electronics and Electrical Communication Engineering from I.I.T. Kharagpur in 1972, the M.Tech. and Ph.D.(Tech.) degrees in Radio Physics and Electronics from the University of Calcutta in 1974 and 1990 respectively. He is presently a Professor in the Department of Radio Physics and Electronics and also acting as the Deputy Co-ordinator of the Centre of Advanced Study in Radio Physics and Electronics, Calcutta University from April 2011, Director (Hony.), UGC-Networking Resource Centre in Physical Sciences, Calcutta University, Director (Hony.) of the Centre for Teleinfrastruktur (CTIF) – India. His research interests include Gunn-diode Oscillators, Power Combiners, Microwave Properties of Conducting Polymers and Rubbers, Electromagnetics, Speech Recognition and Processing, Biomedical image Watermarking. Dr. Ghosh is a life member of the Society of EMC Engineers (India);

Dr. Mahua Bhattacharya is an Associate Professor since December 2006 of ABV Indian Institute of Information Technology and Management, an MHRD Institute of Govt. of India. She had her B.Tech and M.Tech degree from the institute of Radio Physics and Electronics, Calcutta University. She worked as a research scientist at Indian Statistical Institute, Calcutta from 1995 till 2000 Calcutta and got her Ph.D degree on medical image processing in 2001. Her area of specialization is based on Image Processing, Pattern Recognition, Computer Vision, Soft Computing. She works in the area of Multimodal Medical Image Analysis, Medical Image Fusion, Image Registration, Mammographic Image Analysis, Classification of Tumor/Cancer Lesion in CNS, Study of Bone Degeneracy. She was recipient of Frank George award for her paper entitled - Cybernetic Approach to Medical Technology: Application to Cancer Screening and Other Diagnostics' WOSC the World Organization of Systems & Cybernetics, UK. She has published more than 120 papers in International journals and conference proceedings and as book chapters. She is a selected member of Irish Pattern Recognition and Classification Society, 2006, UK and member of International Association of Pattern recognition (IAPR) and coordinating member of National Brain Research Centre (NBRC). She is invited Speakers in different international and national forums and serves as Program Chairs, Session Chairs and Advisory Technical

Committees of International Conferences. She is reviewers of IEEE, Elsevier, Springer and Wiely journals. She is also Principal Investigator of various Govt. sponsored research projects.

How to cite this paper: Subhajit Koley, Koushik Pal, Goutam Ghosh, Mahua Bhattacharya,"Secure Transmission and Recovery of Embedded Patient Information from Biomedical Images of Different Modalities through a Combination of Cryptography and Watermarking", IJIGSP, vol.6, no.4, pp.18-31, 2014.DOI: 10.5815/ijigsp.2014.04.03