Challenges and Prospects of Blind Spread Spectrum Medical Image Watermarking

[1]Eze Peter U., **[2]Udaya Parampalli**
[1,2]Department of Computing and Information Systems
University of Melbourne
Melbourne, Australia
[1]peze@student.unimelb.edu.au
[2]udaya@unimelb.edu.au

[3]Iwuchukwu Uchechi C., **[4]Onuekwusi Nnaemeka**
[3,4]Department of Electrical/Electronic Engineering
Federal University of Technology Owerri
Imo State, Nigeria
[3]uchechi.iwuchukwu@futo.edu.ng
[4]nnaemeka.onuekwusi@futo.edu.ng

Abstract*— Spread Spectrum Watermarking is an emerging area in digital information security. Building from the security provided by this technology in Communication Engineering, one could leverage the same concept to hide patient data securely in a medical image to be transmitted to a remote physician for diagnostic purposes. Spread spectrum is known to hide information as low-power noise using coding sequences with high autocorrelation but low cross-correlation. This ensures that only recipients with the appropriate key can decode the information hidden in the cover and also that more than one user could hide data in the same cover without significant interference. Attackers would find it difficult to decode or even destroy the hidden information without destroying the cover itself. However, there are certain challenges such as amount of information that could be hidden, the fidelity of the information retrieved after unintentional processing and possibility of added information reducing the diagnostic quality of the medical image. In this research, both scholarly survey and experimental evidence were employed to investigate the challenges and possible solutions to utilizing spread spectrum watermarking in the area of medical data hiding for Telemedicine. It was found that even though medical images with higher pixel depth have high watermark imperceptibility at high embedding rates, their susceptibility to noise is higher such that detection accuracy for blind watermarking is often below 100% for spatial domain watermarking. It is thus concluded that more adequate pre-processing and embedding strategy are needed in order to increase detection efficiency for robust watermark embedding for medical images with high embedding rates.

***Index Terms*—Blind Watermarking; spread spectrum; medical; image.**

I. Introduction

After financial data, the next class of data that require high security and privacy are the medical data of an individual. This is because it also contains sensitive data that could either lead to financial details or data that could turn out to be scandalous if divulged. The advent of Information and Communication Technology (ICT) has brought about e-Health and telemedicine as one of its applications, where Electronic

Medical Records (EMR) and medical image scans are transmitted electronically just as financial data. Hence, apart from data encryption, another layer of security would be beneficial to give more protection to medical data and EMR. Both Steganography and invisible digital watermarking are information hiding techniques in which a message is hidden in a cover such as text, image, audio or video to avoid detectability. However, it is very important to differentiate between these two technologies for the purpose of this paper. In steganography, the cover is used as a mere carrier of the message and is not of special importance to the sender or the receiver. On the other hand, in watermarking, the message hidden in the cover is used to give more value or validity to the cover and make it more useful for both the sender and the receiver. Hence, the requirements of steganography and digital watermarking cannot be the same in practice. A more detailed discussion on the difference between steganography and watermarking can be found in [1].

Spread Spectrum (SS) is a modulation technique that tends to utilize transmission bandwidth that is much larger than that of the modulating information. This is achieved by reducing and spreading the energy of the information across various channels with a noisy pseudorandom sequence in the entire carrier bandwidth [2]. The major aim is to reduce the possibility of an attacker detecting, intercepting or jamming the information transmitted in the entire band. In practice, this is done by ensuring that the message does not have a distinguishable peak from the rest of the noise signal in the entire wideband. This leads to higher information security than other modulation and transmission techniques. In the watermarking perspective, the pseudorandom noise is used to spread the hidden data across the carrier cover. For medical images, the idea is to embed the Digital Imaging and Communications in Medicine (DICOM) Protocol header and other necessary EMR of a patient into the medical image, such as computed tomography (CT), magnetic resonance imaging (MRI), ultrasound scan etc., before its transmission for interpretation and diagnosis in telemedicine. Only a physician with the appropriate key can extract the patient information on reception. While on transit, interception and attack on the medical image could remove part of the hidden data but not all, unless the entire image is destroyed. Hence, the idea is to have an extra layer of security for telemedicine.

The concept of blind watermarking is inevitable for telemedicine. With blind watermarking, the recipients will not require the original cover data or originally embedded information in order to extract the watermark [2]. It is obvious that each scan is a new set of data that the receiving medical expert would not have in advance. Hence, private non-blind watermarking, where both sender and receiver have the same cover data for embedding and extraction of information, will not be possible or sensible in telemedicine. Hence, the security and integrity of digital watermarking in telemedicine will rely on the accuracy, efficiency and security of the embedding algorithm, security keys and other parameters.

The purpose of this paper is to survey the challenges and prospects that would enhance the use of Spread Spectrum Watermarking for medical images in telemedicine. The major parameters to consider include watermarking (steganographic) capacity and imperceptibility (diagnostic degradation).

This paper is organised thus: Section II describes a general approach to SS Watermarking; Section III reviews the requirements for medical image watermarking and compares how different researchers met some of these requirements while Section IV presents specific work of various researchers in SS Watermarking in telemedicine. Section V analyses the various challenges facing the use of SS for medical image watermarking while Section VI suggests the prospects and possible solutions. Section VII concludes the work while pointing to directions for further research.

II. A Generalized spread spectrum watermarking system

The embedding functions generally used for spread spectrum watermarking could be additive, multiplicative or exponential [3, 4]. The general block diagram of an SS watermarking system is shown in Fig. 1 below. The embedding function is the main component of the embedder/encoder/modulator sub unit.

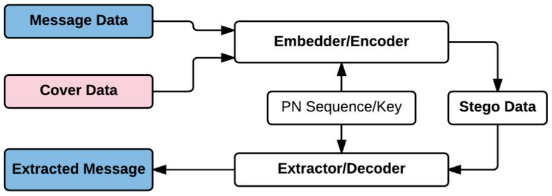


Fig. 1. General SS watermarking.

In Fig. 1, the stego data is assumed to have been encoded onto a transmission channel to a new destination where the original cover and embedded message are needed. The PN sequences for embedding and extraction (spreading and despreading implied as well) needs to be synchronised between the sender and the receiver.

According to [3], the function used to implement the embedder/encoder influences the most important characteristics of an embedding algorithm: robustness, imperceptibility and capacity. The commonly used embedding functions could be additive, multiplicative or exponential as given in (1) – (3) respectively.

$$Y_{ij} = X_{ij} + \alpha W_{ij} \quad (1)$$

$$Y_{ij} = X_{ij}\left(1 + \alpha W_{ij}\right) \quad (2)$$

$$Y_{ij} = X_{ij} e^{\alpha W_{ij}} \quad (3)$$

Y_{ij} is the individual elements of a watermarked data, X_{ij} is the individual elements of the original cover data, W_{ij} is the generated pseudorandom noise signal while α is called the *embedding strength*. The choice of an embedding function and embedding strength determines the success of an embedding algorithm. The embedding function and embedding strength determine to what level the added watermark modifies the values of the pixels or transform domain coefficients of the original cover data. The design of the embedding strength largely depends on the purpose of watermarking (robust, fragile, semi-fragile) and human visual system; it could be according to localised or global regions in the cover data.

It should be noted that the actual information to be transmitted has not been encoded by any of (1) – (3). The encoding of the actual information is determined by the way in which the information will be retrieved. Generally, information retrieval (final message) in SS watermarking is by a linear correlation between Y_{ij} (or its attacked version) and W_{ij}. Hence, if the message bits to be embedded are represented by a vector $S_i = \{0, 1\}$, then to ensure a good correlation during extraction, each of the terms W_{ij} in (1) – (3) will be multiplied by $(-1)^{S_i}$ [5]. Thus in (1), for example, a 0 is encoded as $Y_{ij} = X_{ij} + \alpha W_{ij}$, while a 1 is encoded as $Y_{ij} = X_{ij} \alpha W_{ij}$. Hence, a complete additive embedding function is given as (4) below:

$$Y_{ij} = X_{ij} + \alpha W_{ij} \left(-1\right)^{S_i} \quad (4)$$

In spread spectrum embedding, there is actually no one-toone correspondence between S_i and W_{ij}. Many bits of W_{ij} will be used to embed a single bit, S_i. Thus, in a sub-block embedding process, block W_i could be used to embed S_i. This is actually what information spreading is all about. In this case, the extraction of a bit, S_i¢ , follows the process described in [26] as (5) below.

$$S_i' = \begin{cases} 0, & Corr(Y_{ij}, W_{ij}) > 0 \\ 1, & Corr(Y_{ij}, W_{ij}) < 0 \end{cases} \quad (5)$$

Corr( ) is the statistical linear correlation between two variables. The challenge of Spread spectrum watermarking is to design code sequences that has proper correlation properties and to choose appropriate embedding strength in order to optimize robustness, imperceptibility and capacity. The choice of coding scheme and code length is a separate area of research. Also, for practical purposes, it has to ensure compliance with Kerckhoff's second principle of Cryptography [6] in which the algorithm is known to the enemy but the key is strong or secret enough to ensure that the embedded message cannot be retrieved by the enemy.

It should be noted that some SS watermarking systems utilize two keys: watermark generation key and watermark embedding key. The generation key is used to generate the pseudorandom sequence while the embedding key determines on which locations in the cover the watermark is actually embedded. This provides two-level security in some applications.

The general blind extraction mechanism for SS is by correlation between the filtered watermarked signal and the pseudo noise code. This could be extended to thresholding and other error analysis methods for better watermark detection and extraction fidelity [26]. The general representation of a blind extraction method is shown in Fig. 2 below. For most blind extraction techniques, the correlation method of various adaptations is used.

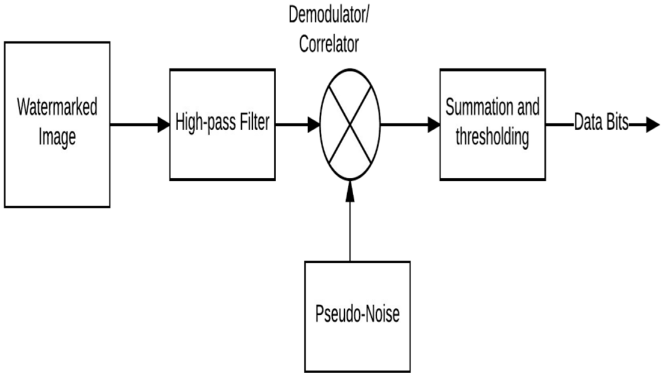


Fig. 2. Blind Watermark Extractor.

Just as shown in Fig. 1, the pseudo-noise used during embedding should be synchronised with the one used in Fig. 2 for extraction. De-synchronisation problems can be detected with a sliding correlator placed between the high pass filter output and the pseudo-noise signal [11].

With spread spectrum, EMR will be added to a medical image in either the frequency or the spatial domain.

III. REQUIREMENTS FOR MEDICAL IMAGE WATERMARKING

The interpretation of pixel changes in a medical image is of health importance and thus the alteration of even a few pixels may lead to a different diagnosis. Hence, the level of image processing that will need to be done on a medical image needs to be carefully determined and applied. This implies that imperceptibility is an important requirement [12, 17, 21]. This is not just to reduce steganalytic attacks but to preserve diagnostic qualities of the medical image.

Generally, there is the option of embedding a watermark reversibly or irreversibly. The chosen method is determined by level of degradation allowable to maintain accurate diagnosis and on what the watermark is meant to achieve: annotation or authentication. Medical images are divided into Region of Interest (ROI), which is essential for patient diagnosis and Region of Non-Interest (RONI), which is not used for diagnosis. On some images, however, the ROI is large and the RONI is small. In most applications, the watermark for authentication is placed on the ROI and often made reversible to ensure zero degradation after authentication. The annotation data that contains EMR are usually embedded in a robust manner in the RONI. The challenge is if the RONI is large enough to accommodate equivalent DICOM header information and other EMR. In this case, it is necessary to establish what level of degradation will render the ROI ineligible for accurate diagnosis. This is in a bid to establish if some annotation watermarks can be added in the ROI region as well. Hence, even though [12] identified reversibility as one of the requirements of medical image watermarking, the purpose (authentication or data hiding), region of embedding and computational complexity are the main determining factors for this requirement.

Certain data privacy regulations guide the security of patient information. *ISO 27799:2016* relates to guidelines in organisational information security standards. More specific to health information security is its guideline on how to implement *ISO/IEC 27002* for health informatics [9]. In USA, the Health Insurance Portability and Accountability Act (HIPPA) of 1996 implies all medical data belonging to an individual should be confidential, available and of high integrity/reliability [10, 17, 21]. Thus, medical image watermarking, apart from having to observe the general digital watermarking requirements of capacity, imperceptibility and robustness [20, 21], will also have to comply with legal requirements [22] and diagnostic/clinical validity [23,24]. Special requirements and constraints will be necessary if the medical image to be watermarked will be used for autodiagnosis. This is because there is always a conflict between the image processing requirements for computer-based autodiagnosis and the watermarking requirement of robustness. This becomes more complex when both watermarking for authentication and watermarking for annotation (data hiding) are implemented on the same medical image [12].

For embedding of EMR, it is important to establish what capacity of actual information could be hidden. As more doctors' notes may need to be embedded together with conventional DICOM header information, it will be interesting to estimate the amount of characters that a payload could be made of. The survey of watermarking techniques for medical images carried out in [12] compared the work of various researchers in various ways but not in terms of embedding capacity. In Table 1 below, existing capacities (using the researchers mentioned in [12] and other researchers) achieved by various researchers were compared. Eight bits per ASCII (American Standard Code for Information Interchange) code character was used to compare the amount of equivalent characters hidden or watermarked.

Table 1: Comparison of Embedding Capacities in Medical Images.

Author(s)	**Modality**	**Purpose**	**Region**	**Method**	**Capacity**	**Characters**	**PSNR (dB)**
Memon *et al* [13]	CT	Authentication	RONI	LSB	64Kb	8,192	51.00-60.00
Zain and Clarke [14]	US	Integrity Authentication	RONI	LSB	510Kb	65,280	24.96-31.70
Wakatani [15]		Data Hiding	RONI		5.9Kb	755	22.36
Al-Quershi and Khoo [16]	MRI, US, CT, CR	Authentication Data Hiding	ROI, RONI	DE DWT	413.8Kb	52,966	65.20-69.70
Maity and Maity [17]	X-ray, CT MRI	Authentication Data Hiding	ROI, RONI	RCM IWT SS	126Kb	16,235	44.34- 45.89
Pan *et al* [19]	X-ray, US, MRI, PET	Data Hiding	Whole	DWT	45Kb(0.2bpp)	5,760	51.10
Kumar *et al* [20]	MRI, US	Data Hiding	Whole	SS	1Kb	128	30.14 - 41.41
Naseem *et al* [21]	US	Authentication, Data Hiding	ROI RONI	SS, RNS Chaos	2.69Kb	344	-

CT=Computed Tomography, US=Ultrasound Scan, MR = Magnetic Resonance Imaging, LSB= Least Significant Bit, DE = Difference Expansion, DWT =Discrete Wavelet Transform, RCM = Reversible Contrast Mapping, IWT = Integer Wavelet Transform, SS = Spread Spectrum.

It is worthy of note that the capacities in Table 1 should not be considered in isolation. Peak Signal-to-Noise Ratio (PSNR) is a measure of statistical imperceptibility between an 'attacked' image and a reference image. The imperceptibility achieved with these capacities are of great importance in medical image watermarking. Their hiding capacities at best PSNR were recorded here. In medical image watermarking, high imperceptibility is needed and thus specific PSNR value and hiding capacity may need to be established either as a general benchmark or for specific applications. Table 1 is a mere comparison on loosely defined data with no common base for experiments by various researchers. It would be better if all researchers could express information hiding capacity in terms of bits per pixel (bpp).

Also, the size, depth and number of channels of the cover into which the message is embedded are also determining factors. In most of the work, these were not clearly stated. Hence, there is a need to establish a common base for comparison. Most public medical images for research are sized at 512x512, single channel and 8-16 bits deep.

IV. PREVIOUS WORK ON SPREAD SPECTRUM IN TELEMEDICINE

In recent times, some researchers began to explore the theories and practice of utilising SS for medical image watermarking. This is as a result of the success recorded by SS in military communication systems in terms of security and robustness [4, 7]. However, digital images in general and medical images in particular, do not have that much bandwidth and flexibility as a conventional telecommunication channel. Hence, the need to study the application of SS in medical images in more details.

The researchers in [17] applied SS for the robust watermarking of X-ray, brain MRI and head CT scan. They used a polygon ROI and embedded logos of 32x32 into 512x512 cover medical images. They combined reversible and robust watermarking through reversible contrast mapping and Integer Wavelet Transform Spread Spectrum (IWT SS) watermarking respectively. They got best performance using X-ray cover where they achieved PSNR of 44.34 at an embedding rate of 0.491*bpp*. However, the watermark extraction from the RONI was not non-blind. The correlation equation had the original cover image as one of the parameters for extraction. Whereas non-blind extraction is more efficient as it eliminates the host cover energy interference with the watermark [18], it is very unlikely that the receiving hospital would have the cover medical images beforehand in order to enable non-blind extraction.

An attempt on multi-access SS for medical image watermarking was implemented by Kumar et al in **[20]** on MRI and US image covers of 512x512. They studied the effect of variation in gain factor, level of decomposition of DWT sub-bands, type of wavelet filter used and the type of medical image modality on the performance of their algorithm. They achieved a very low embedding rate of 0.0039*bpp* at a PSNR of 41.412dB. Their highest embedding rate was 0.0244, which was achieved at PSNR of 30.138 dB. Though the embedding rates and PSNR are relatively low, their algorithm was highly robust against various attacks which they simulated on the watermarked image. They utilised the Gaussian N (0, 1) pseudo-noise watermark distribution for multi-user embedding. That is a watermark distribution with 0 mean and variance of 1. Their SS watermarking was fully blind and thus is a better model for tele-radiology.

A Spread Spectrum invertible watermarking system utilising Residue Number System (RNS) and Chaos was implemented by Naseem et al in [21]. They used a ROI/RONI mechanism to achieve authentication and data hiding schemes. Their test cover image was a 194x259 US image and the watermarks were a 50x50 image and a 256-bit image hash. Robust watermarking of the logo was done in the RONI, while fragile watermarking of the hash was done in the ROI. They also performed various types of attacks on the watermarked image. Their study, however, focused on robustness rather than perceptibility. No data on PSNR was given.

V. CHALLENGES OF BLIND SPREAD SPECTRUM WATERMARKING

There are different factors that mitigate against the use of SS watermarking. Some are general to SS while others are specific to blind SS watermarking.

A. Embedding Strength or Gain Factor

Imperceptibility of a watermark is a major requirement for medical images. This is often set by the embedding strength chosen [8]. However, the study carried out in [20] shows how the embedding strength affects watermarked image quality. This study shows that increase in embedding strength increases extracted watermark fidelity but decreases the PSNR and thus the imperceptibility of the embedded watermark. This conflict between robustness and imperceptibility is a major problem where a large watermark needs to be imperceptibly embedded into the entire medical image without separation into ROI and RONI. This type of embedding is often considered where ROI occupies a very large portion of the entire medical image.

B. Spreading Factor (SF) Vs Steganographic Capacity

Spreading factor is used to determine how wide a message is spread within the cover. This, in turn, determines the amount of actual message (as opposed to pseudo noise) bits that could be embedded. SF is defined as:

$$\text{SF} = \text{chip rate/symbol rate} \tag{6}$$

In binary, SF is the number of spreading bits used to encode one bit of information. A chip is the shortest modulated signal by a symbol (0 or 1). For example, if a message bit is spread with a 63-bit gold code then the SF =63. In simple terms, SF is the length of the spreading code. For GPS systems, an SF of 1024 is typical while typical SF in CDMA systems range from 4 to 512 [7].

However, it should be noted that the higher the SF, the more secure the system but this reduces the capacity of actual data hidden by SF as well. Hence, finding the best trade-off between security and hiding capacity remains a challenge.

C. Multiple Embedding

As more than one medical expert could work on a medical image, there is a need that each of them has a footprint on the image by way of recording their diagnostic findings and recommendations. This requires data generated by different medical experts to be embedded. With the constraints already posed by both embedding strength and spreading factor, coupled with the increased potential for interference among the data relating to different diagnostic activities, it becomes challenging to embed multiple data using SS. The research in [26] shows that for traditional SS watermarking, there is no zero-correlation (see (5)) even when no data is embedded in a block. More interference is expected with multiple embedding.

D. Widely Varied Computational Complexity

The computational complexity should be low for authorised users but high for attackers. This becomes more important for emergency situations. The authorized users require computationally efficient algorithms together with security. As for the attackers, the extraction method without the keys and the steganalytic process should be computationally inefficient and all exhaustive search for extraction should be nearly NP-complete. Also, backdoors should be properly checked to avoid easy access for intentional attackers. Achieving these contrasting requirements simultaneously with a Kerckhoff-based public algorithm has remained a challenge.

E. Detection Efficiency and Reliability

Blind detection is prone to host energy interference [18] and de-synchronisation problems between the sender and the decoder. Also, accurate modelling of both the cover image and the embedded spreading code is very important for blind SS watermarking. This is even more important when multichannel (multiple users) detection is required. This problem of detection efficiency is really high in DICOM images with more than 8-bit pixel depth. Fig. 3 and Fig. 4 show the detection accuracy for 0-bit and 1-bit watermarks in a collection of 4096 sub-blocks in Lena and Lumbar MRI image respectively.

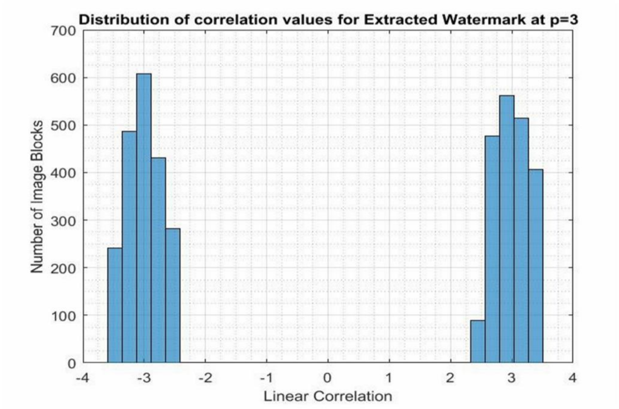


Fig. 3. Watermark detection in 8-bit Lena sub-blocks.

There is a clear detection of 0 and 1 bits at correlations (***p***) centred at -3 and 3 respectively. The same algorithm was run on 13-bit DICOM image and the result in Fig. 4 was obtained.

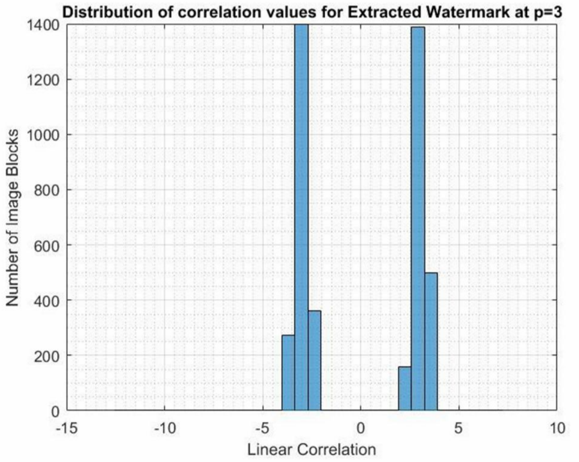


Fig. 4. Watermark detection in 13-bit DICOM image.

Though it may seem that all 4096 bits were extracted in case of Fig. 4, 4092 bits out of the 4096 (***99.9%***) were extracted while the entire 4096 were successfully extracted in the case represented in Figure 3. Hence, though four false negatives are low, in the case of text embedding, a very different character could result. The false negative possible resulted from pixel overflow and/or underflow due to high embedding strength required by some sub-blocks to maintain a correlation coefficient that is farther away from zero. A little histogram equalisation before embedding could solve this problem. However, for medical images, this may not be allowed in the ROI. Hence, controlled or selective embedding could be used in such case.

F. Scalability Issues

The bandwidth of all embedding media is very limited. They are limited by the size of the image, bit depth and domain of embedding (Spatial or transform). For medical images, there are even more limitations poised by the need to preserve the diagnostic quality of the medical image and the region of embedding being used (ROI or RONI). These general and specific limitations have reduced the number, type and purpose of applications to which SS medical image watermarking could be applied. For instance, a medical image with large ROI will not benefit much from robust data hiding in the RONI but could be maximized for medical image integrity in the ROI.

Furthermore, there is a general belief that the more complex an algorithm, the more difficult it would be for an attacker to break. This has led to algorithms with several loops, which take a very long time to execute especially in a large-scale watermarking environment. Hence, many watermarking algorithms have ended up as experimental designs and prototypes but cannot be implemented for clinical use without further redesign. Thus, apart from the correctness of an algorithm, watermarking algorithm designers need to understand that scalability and efficiency are also important for practical purposes. This is even more important with medical image watermarking especially for medical emergencies.

G. Inaccurate Modelling of Cover Data

Different assumptions have been made in modelling the cover image itself. Cover images have been modelled as having normal and independent and identical distribution (i.i.d), Guassian distribution, Laplacian and Markov chain distribution. The use of a wrong model could hamper adequate design and analysis of spread spectrum based watermarking systems. Accurate modelling is required in both frequency and spatial domain of embedding.

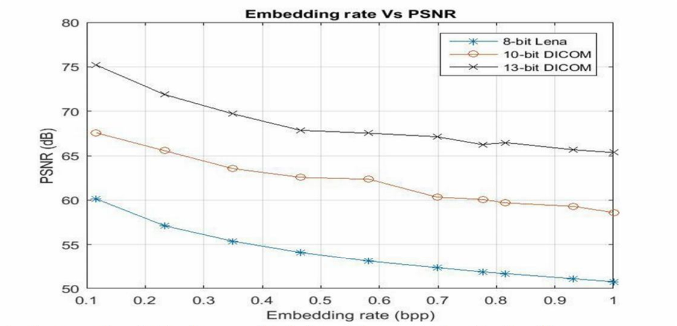
VI. Prospects of Spread Spectrum for Medical Image Watermarking

It is obvious that the requirement for high security places a lot of constraints on the amount of data that could be hidden using SS watermarking. How then can both higher security and high Steganographic capacity simultaneously in medical images be achieved? The following possibilities were explored:

A. Multichannel Embedding through highly Orthogonal Eigen-based Spreading Codes

Code division multiplexing in conventional CDMA systems enables many users to transmit in the same channel using different codes. The success of this communication system is dependent on the independence and/or low correlation of the codes assigned to different users. The design of a highly orthogonal code that isolates a user in the presence of multiple noise sources and interferences will help to increase the hiding capacity in images using spread spectrum.

Akansu and Poluri in [25] showed how the Karhunen–Loeve Transform (KLT) codes could outperform the widelyused Gold and Walsh codes. The drift into eigen-based code design will eliminate the problems of limited code length, poor performance and the number of available codes [25]. Further work by Gu *et al* in [27] proposed an improved performance eigen-based spreading sequence for multi-user applications when designed using Uniform Orthogonal Transformations (UOT). These exploits for multi-user satellite systems and CDMA systems could be adapted for SS watermarking systems, especially in the transform domain.



B. Exploring the 3-D slices of Medical Images for Embedding

Most medical image scans are made up of slices and volumes. There exist 2-D, 3-D and 4-D medical images. Spatially, this provides opportunities for data embedding. As medical image watermarking is most suitable for already processed medical images, the prospect of digital image watermarking would utilize both the natural features and modified medical image multidimensionality to provide more avenues for higher embedding and distortion/security management.

The Medical Imaging and Technology Alliance (MITA) in [28] has posited that advancements in 3-D and 4-D medical imaging would improve visualization while minimizing distortion. The minimized distortion feature could be explored for improved capacity, security and imperceptibility during the watermarking of the same image.

C. Multi-level Security for smaller SF

If more data needs to be embedded, then smaller SF will be used. To avoid compromising security, a second layer of security such as encryption and block chaining could be used. In such a case, the bit that could be possibly recovered from each block would not be the direct message bits. In this case, a bit-by-bit encryption method (character substitution) would be used so as not to increase the data payload after the encryption process.

D. Higher Pixel Depth for Medical Images

Fig. 5 shows the variation of PSNR values at various embedding rates for 8-bit Lena image, 10-bit and 13-bit DICOM images. The 13-bit DICOM image showed the best quality while the 8-bit Lena image showed the worst quality at the same embedding rate. Most medical image scans contain slices and frames and thus have more bit depths per pixel or voxel. This provides hope for higher embedding capacity without compromising quality in medical images especially in the spatial domain. Hence, if the problem of extraction accuracy is solved by designing an accurate correlation method with the high pixel depth medical images, Figure 5 has shown that medical images have higher PSNR than 8-bit Lena images.

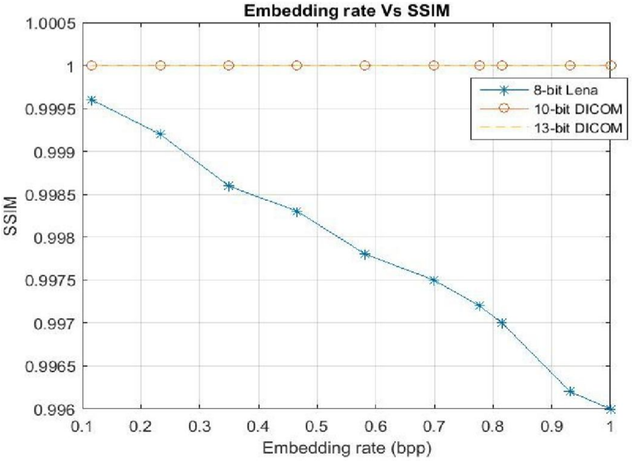


Fig. 5. PSNR for various Pixel Depths.

In Fig. 5, the PSNR of a 13-bit DICOM image still remains above 65dB at the embedding rate of 1.0 bpp as opposed to that of Lena that is a little above 50 dB at the same rate. In this experiment, the performance of 13-bit DICOM medical image still remained better even though its entropy is far below that of Lena. In terms of perceptual (visual) imperceptibility measured using Structural Similarity Index (SSIM), Figure 6 shows that medical images are very promising even at embedding rates higher than 1bpp in the spatial domain.

Fig. 6. Perceptual performance in DICOM and Lena.

Whereas the quality of Lena decreases rapidly as embedding rate increases, that of Medical images of 10-bit and 13-bit pixel depth remain constant at the maximum value of 1. Hence, medical images have high embedding rate at high statistical and visual imperceptibility.

E. Efficient Algorithm Design

Complex software systems require good knowledge of the problem domain as well as strategic software engineering principles. Watermarking algorithm designers need to think of scalability. The experimental approach provides a working algorithm but long-term use requires efficient and scalable algorithms for real-time use in tele-medicine. This implies considering the worst-case scenario in terms of length of time it takes to embed/extract the maximum capacity of the watermarked image.

The fact that most security professionals have a background in computer science brims a hope that watermarking algorithm designers would take advantage of the problem domain as well as the principles of modern software engineering (not just software development) to develop watermarking algorithms that would be efficient enough to run with average processor speed and memory within the required time for medical diagnosis and treatment especially during medical emergencies. Special attention should be given to loops, recursive functions, modular design and memory management techniques.

Detection efficiency in SS systems will be achieved by the use of highly orthogonal codes and by the removal of mean as mentioned in [26]. Also, advancements in statistical modelling and adaptive embedding for host images will lead to efficient detection. Design for appropriate of embedding strength will also help to improve detection accuracy and efficiency.

F. Multiple but Efficient Key Management Strategy

In the long run, the development of Quantum Key Distribution (QKD) and the resultant increase in network speed would ensure both real-time and secure transmission of keys not minding the length and number [29]. QKD allows a large number of key bits to be transmitted securely and at high speed even in the presence of an adversary. It basically works through quantum mechanics and polarization of light. The concepts of QKD and its vulnerabilities are discussed in [30]. It is obvious that cryptography and steganography are complementary though some idea from cryptography may not be implemented as-is in steganography and digital watermarking.

VII. CONCLUSION

Medical images have high prospects of being secured through digital watermarking due to their higher pixel depth, voxel representation and higher embedding capacity at low perceptibility. However, most of them have low entropy and are thus affected more by noise, including the internal noise due to the cover image itself. Spread spectrum technology offers increased security but reduces embedding capacity due to the fact that higher spreading factor provides higher security while reducing embedding capacity. In order to attempt to solve these problems, highly orthogonal embedding codes and adequate pre-processing are required. Also, the transform domain of hiding should be investigated as the rounding problems associated with spatial domain is not the case. Multiaccess embedding strategy adapted from CDMA should also be explored to increase the embedding rate and compensate for what was lost by higher spreading factor. A dynamic method of designing embedding strength to optimize robustness and imperceptibility while achieving maximum hiding capacity is also recommended. Finally, controlled embedding strategies should be adopted to avoid embedding in sub-block with very poor watermarking qualities.

References

[1] I. Cox, M. Miller, J. Bloom, J. Fridrich and T. Kalker. *Digital Watermarking and Steganography.* Edited by I. Cox et al., Elsevier Science, 2007. ProQuest Ebook Central.

[2] V. Dhore and P.M Arfat. "*Secure Spread Spectrum Data Embedding and Extraction*" In International Journal of Science and Research, ISSN:2319-7064.Vol 4(1), 2015, Pp 743-747.

[3] F. Kammoun, A. Khalfallah and M.S Bouhlel. "New Scheme of Digital Watermarking Using an Adaptive Embedding Strength Applied on Multiresolution Filed by 9/7 Wavelet". Wiley Periodicals, Inc., 2007.

[4] S. Ghoniemy, O.H Karam and O. Ibrahim. "R*obust and Large Hiding Capacity Steganography using Spread Spectrum and Discrete Cosine Transform*" In *International Journal of Image Processing and Visual Communication,* ISSN: 2319-1724: Vol 1(4), 2013.

[5] Z. Shahid, M. Chaumont and W. Puech "Spread Spectrum-based Watermarking for Tardos Code-based Fingerprinting for H.264/AVC Video". *University of Montpellier* II, 2011.

[6] S. Mrdovic and B. Perunicic. "Kerckhoff's Principle for Intrusion Detection" [online] http://people.etf.unsa.ba/~smrdovic/publications/Networks2008_Mrdovic_Perunicic.pdf accessed 23/02/2017.

[7] National Instruments. "*Understanding Spread Spectrum for Communications*" . [online] http://www.ni.com/white-paper/4450/en/ accessed 2nd March, 2017.

[8] J. Zhong. *Watermark Embedding and Detection*. Ph.D Thesis, Department of Computer Science and Engineering, Shanghai Jiaotong University, 2007.

[9] ISO 27799:2016, *Health informatics -- Information security management in health using ISO/IEC 27002.* [online] http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=62777 accessed 3rd March, 2017.

[10] US Department of Health and Human Services. "*The HIPPA Privacy Rule*" [online] https://www.hhs.gov/hipaa/for-professionals/privacy accessed 3rd March 2017.

[11] M. George, J. Chouinard and N. Georganas. "Spread Spectrum Spatial and Spectral Watermarking for Images and Video". *School of Information Technology and Engineering, University of Ottawa Canada*. [online] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.30.8246&rep=rep1&type=pdf retrieved 3rd March, 2017.

[12] S.M Mousavi, A Naghsh, and S.A.R Abu-Bakar. "Watermarking Techniques used in Medical Images: A Survey" In *Society for Imaging Informatics in Medicine*, May 2014. DOI: 10.1007/s10278-014-9700-5

[13] N.A Memon and S.A.M Gilani. "Watermarking of Chest CT scan Medical Images Authentication" In *Journal of Computer Mathematics* 88(2): Pg 265-280, 2010.

[14] J.M Zain and M. Clarke. "*Reversible Region of Non-interest (RONI) watermarking for Authentication of DICOM images*" In *International Journal of Computer Science and Network Security*, 7(9): pp 19-28, 2007.

[15] A. Wakatani. "*Digital Watermarking for ROI Medical images by using compressed signature image*" *Proceedings of the 35th Annual Hawai International Conference*, pp 2043-2048, 2002.

[16] O.M Al-Quershi and B.E Khoo. "Authentication and Data Hiding using a hybrid ROI-based watermarking schemes for DICOM images" In *Journal of Digital Imaging*, 24(1), pp 114-125, 2011.

[17] H.K Maity and S.P Maity. "*Joint Robust and Reversible Watermarking for Medical Images*" In 2nd *International Conference on Communication, Computing and Security, Procdia Technology* 6, pp 275 – 282, 2012.

[18] P. Meerwald and A. Uhl, "*Scalability evaluation of blind spreadspectrum image watermarking*". *Department of Computer Sciences, University of Salzburg, Austria.*

[19] W. Pan, G. Coatrieux, N. Cuppens and C. Roux, "*An Additive and Lossless Watermarking Method Based on Invariant Image Approximation and Haar Wavelet Transform*" In *32nd Annual International Conference of the IEEE EMBS Buenos Aires, Argentina*, August 31-Sept. 4, Pg 4740 – 4743,2010.

[20] B. Kumar, H.V. Singh, S.P Singh and A. Mohan, "*Secure SpreadSpectrum Watermarking for Telemedicine Applications*" In *Journal of Information Security* Vol 2,Pp. 91-98, 2011.

[21] M. Naseem, I. Qureshi, M. Muzaffar and A. Rahman, "Spread Spectrum based Invertible Watermarking for Medical Images using RNS and Chaos" In *The International Arab Journal of Information Technology*, Vol.13(2),pp. 223-231, 2016.

[22] G. Coatrieux, C. Quantin, F. Allaert, B. Auverlot and C. Roux, "Watermarking – a new way to bring evidence in case of telemedicine litigation" In *European Federation for Medical Informatics*, DOI: 10.3233/978-1-60750-806-9-611, pp. 611-615, 2011.

[23] H. Nyeem, W. Boles and C. Boyd, "*A Review of Medical Image Watermarking Requirements for Teleradiology*" In *Journal of Digital Imaging*, 26(2), pp. 326-343, 2013.

[24] G. Coatrieux, L. Lecornu, C. Roux and B. Sankur, "*A Review of Image Watermarking Applications in HealthCare*" In *Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 4th February, 2006. DOI: 10.1109/IEMBS.2006.259305

[25] A.N Akansu and R. Poluri. "*Design and Performance of KarhunenLoeve Transform for Direct Sequence CDMA Communications*" In *IEEE Signal Processing Letters* Vol. 14, No. 12, Pp. 900-903, December 2007.

[26] T.T Nguyen and H.D Tuan. "*A Modified Spatial Spread Spectrum Method for Digital Image Watermarking*" . 2nd *International Conference on Communication and Electronics*, Hoi an, Vietnam, 4-6 June, 2008.

[27] N. Gu, L. Kuang, X. Chen, Z. Ni and J. Lu. "*An Eigen-based Spreading Sequences Design Framework for CDMA Satellite System*" In *IEEE 79th Vehicular Technology Conference, Seoul Korea*, 2014.

[28] MITA. "The New wave of Imaging" [online] http://www.medicalimaging.org/imagingforward/3d-4d-and-beyond/ retrieved May 11, 2017.

[29] A.S Tanenbaum and D.J Wetheall . *Computer Networks (5th Ed.)*. Pearson Education Inc., USA, 2011.

[30] M.R Grimaila, J. Morris and D. Hodson. "*Quantum Key Distribution: A Revolutionary Security Technology*" In *International Systems Security Association (ISSA) Journal* Pg. 20-27, June 2012.