An Evaluation of Data Security for Telemedicine Application Development

Hetal N. Rao
PG Research Scholar
Department of Electronics and Communication
RK University, Rajkot, India

Manoj Pandya
Senior Project Scientist
BISAG
Gandhinagar, India

K M V V Prasad
Assistant Professor
Department of Electronics and Communication
RK University, Rajkot, India

ABSTRACT
Digital Communication has made the data transfer and data communication very fast, easy and efficient. In the field of the data security several techniques are used right from the years ago. This includes Cryptography, Steganography and Watermarking techniques. This paper includes the review and comparative analysis of all these three techniques for the field of Image Processing focusing to the Medical Images. As for Healthcare field, security of data is more sensitive and important, we are analyzing for the most suitable technique for this purpose. This review is initial part of the research for developing the application of data security using efficient algorithm that follows the specific and robust transformation technique useful in Telemedicine field.

General Terms
Data Security, Data Hiding

Keywords
Cryptography, Steganography, Watermarking, Copyright Protections, Intellectual Rights

1. INTRODUCTION
According to communication progress, Internet has become the most common source of data sharing and transfer. In this activity of data communication, security, copyright, hacking etc. are the factors upon which we need to focus as well.

Three key technologies are there for it: Cryptography, Steganography and Watermarking (a subcategory of steganography-as per the various researchers). In the modern era of technology, multimedia has become the most popular medium for data transfer. Among various multimedia objects like video, audio, pictures/ images, we are here merely focusing on 'Image'. Therefore this review is more concerning to compare and analyze all above technologies particularly for image data. If take a glance towards the above mentioned three techniques - *Cryptography* is the process of scrambling the information or data using different keys as Public key and Private Key. Cryptography performance is based on two fundamental share which are Encryption and Decryption that are used at sender and receiver end respectively. *Disadvantages of Cryptography* made the basis for development of its next generation, Steganography. In last few years, the research has grown in digital image steganography techniques. The major goal of *steganography* is to achieve security by inserting the data to be hidden within an image by altering the non-data containing pixels. The image after including the secrete message/data to be hidden is called *stago image.* The main difference between cryptography and steganography is that in case of cryptography, only the data content is kept hidden and its existence is not made hidden. Whereas in case of steganography, both the data existence and data itself.

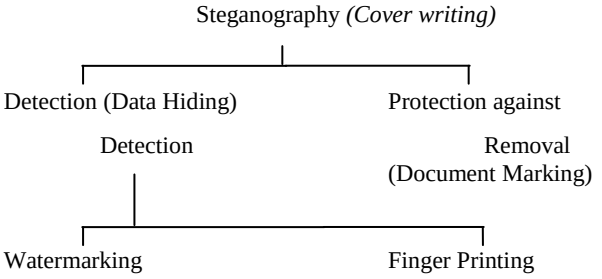

Fig 1: Divisions of Steganography [3]

As per mentioned in the diagram in fig. 1, watermarking is considered as a specific type of the steganography itself. Watermarks are having two types as visible watermark and invisible watermarks. The visible watermarks are as per the name indicates, are having visibility by naked eyes and those, named as invisible, cannot be seen having embedded within the cover image after watermarking. Again there are other classifications of the watermark types as *fragile and semi fragile, blind and non-blind, perceptible and imperceptible* etc.

2. HISTORY
Initially, for the purpose of data security, *Cryptography* had been used from year 1900 in Egypt. At that time, nonstandard methods were used. During 50 - 60 B.C. Julius Caesar used a simple substitution with the normal alphabet in government communications. From 500 – 600 B.C. Hebrew scribes used ATBASH, a reversed alphabet simple solution cipher [5]. Cryptography had been continued with many variations. Steganography has been developed through a longer history of Cryptography.

The origin of *Steganography* is the word '*Steganos'* means covered/secrete. It was developed by Sir Francis Bacon. Initially, it had been originated in Greece. The Greek ruler Histaeus engaged an early version of steganography which involved: shaving the head of a slave, tattooing the message on the slaves scalp, waiting for the growth of hair to disclose the secret message, and sending the slave on his way to deliver the message. The recipient would have the slave's head to uncover the message. The recipient would reply in the same form of staganography [5]. The other early form developed for the *Cryptography.* It involved Demerstus who had written a message for Spartans to warn from the eminent invasions by Xerxes. It was written on wood covered by wax layer which made to seem the tablet being empty but in fact it was containing a secrete message.

Watermarking is more popular technique in today's modern communication for data security especially for the purpose of

proof of ownership, copyrights and other intellectual rights protection. It also hides the existence of the message as Stegonography. This technique had been in use for 700 years back. At that time watermarks were to appear in handmade watermarking. In 1887, legally watermark of two letters was presented as evidence in France [9].

3. LITERATURES

Cryptography is the science of hiding data in some different form than its original one. For this purpose, certain keys are used using them only specific recipients who are having these keys can only decode and retrieve the original message. Two types of keys are used-public key and private key. Using a private key the data is converted into the cipher text and then it is transmitted along the channel and at receiving end it is further decoded using the public key. In this process, there is possibility for data disclosure at the intermediate channel.

In case of *steganography*, it is the art and science of communication in a way that presence of a message is undetectable. ***Jonathan, Patrick, Lau and Robert*** **[3]** have given the comparison of Steganography and Digital Watermarking along with the various types of different types of Steganography. It includes fragile, robust etc. The word, steganography is derived from Greek meaning *as hiding in plain sight*. Both cryptography and steganography are having for confidentiality of data. The word 'confidentiality' means the proof of the sender of the data that it has been sent by the particular person only. In this technique, nobody is able to identify that the communication between two parties is running and hence it is most suitable for the certain applications. Watermarks contain data hidden for the purpose of avoiding its detection and tempering. However they are not always of such imperceptible but are having types, visible watermark and invisible watermark. There are three techniques mentioned for watermark implementation: LSB (Least Significant Bits), DCT (Discrete Cosine Transform) and DWT (Discrete Wavelet Transform).

Peticolas et al. **[5], [3]** proposed a definition of robust watermarking similar to that being used for the music industry.

Samer, Ammar and Putra **[15]**, in their article, mentioned the data hiding through the images for secrete communication, using Steganography. They mentioned the history, development, features and drawbacks of the steganography. Various techniques are shown to be used for data hiding implementation such as LSB, DCT, and DWT etc.

Kaushik, Ghosh and Bhattacharya **[14]** proposed a novel watermarking named, Majority Algorithm Technique that successfully provided the higher PSNR and SSIM values against various attacks as salt and pepper noise and compression of the image.

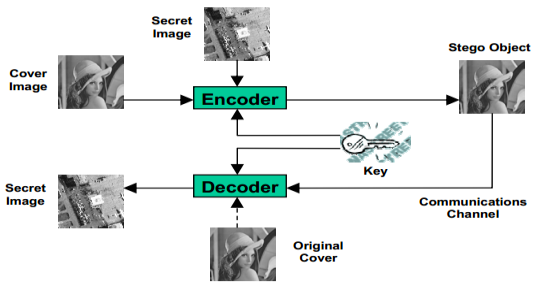

Fig 2: Generic process of encoding and decoding [3]

The above figure shows the general process of encoding-decoding in case of Steganography using mechanism of *key*.

Amirtharajan, Akila and Deepikachowdavarapu **[1]** have given certain methods in frequency as well as spatial domain of steganography in their paper. This includes LSB Substitution, Optimum Pixel Adjustment Procedure, Inverted Pattern Approach (IP), IP method Using Relative Entropy, The Proposed Hiding Streams of 0s and 1s, Pixel Value Differencing (PVD), The Proposed Mod method, The Proposed Mod10 Based method and DCT method. MSE (Mean Square Error) and PSNR (Peak SNR) values are calculated for all the methods.

Abbas, Joan, Kevin and Paul **[2]** show the comparative analysis of the steganography tools. They also included *Steganalysis* which is the method used by steganography to check if the embedded message is secure and the process that has been carried out is successful. A statistical and comparative analysis is done and concluded with the significance of the stenographic tools for JPEG compression as well as considering the *salt and pepper noise* type attack.

Watermarking is concerned mainly with protection of the intellectual property rights, copyrights and authentication of the digital media as per ***Fang and Siu*** **[7]**. It is a process of hiding a data onto a host data or signal for the sake of security provision. It does not require always robustness as that for *Steganography* because watermarks can be visible and also invisible.

Using digital watermarking, copyright information can be embedded into the multimedia data. This is done by using some algorithms. Information such the serial number, images or text with special significance can be embedded. The function of this information can be for copyright protection, secrete communication, authenticity distinguish of data file, etc [8].

4. RESULT ANALYSIS

Here the results of Cryptography, Steganography and Watermarking have been shown, where various functionality and characteristics of all these three techniques are compared.

It can be concluded from the analysis carried out by ***Kaushik, Ghosh and Bhattacharya*** **[14]** that there are various methods for watermarking and the quality of data hiding can be measured in terms of PSNR (peak signal to noise ratio), MSE (mean square error), SSIM (structural similarity index measure). They got the following results:

Table 1 Cover image, Message image and PSNR and SSIM values for the watermarked image [14]

Cover image (256x256)	Message image (16x16)	PSNR (dB)	SSIM
Lena	S logo	42.343	0.9889
Tower	K logo	41.806	0.9781
Fruit	Max Payne logo	41.506	0.9853
Hat	M logo	42.893	0.9798
Baboon	C logo	42.135	0.9621

Where maximum similarity between both cover and watermarked iamge i.e. SSIM = 0.9889 which is nearer to 1.

PSNR = 42.8930 dB that shows the image quality betterment.

Harshita, Ashwani and Satendra **[17]** in their research, proposed the watermarking technology for the protection of the copyrights and obtained the following results for quality of the watermarked image in terms of PSNR and NC:

Table 2 Cover image, Message image and PSNR and SSIM values for the watermarked image [17]

Scale Factor	PSNR	NC
0.01	69.6876	1
0.03	51.8430	1
0.05	46.0586	1
0.07	42.5685	1
0.09	40.0637	1

From the above results it is clear that using watermarking we are able to get the watermarking quality in form of Peak Signal to Noise Ratio as good as 69.69 dB. And the robustness is achieved as closer to 1 as above.

Amirtharajan, Akila and Deepikachowdavarapu **[1]** have measured various parameters like MSE, PSNR, and Time for different steganography and identify several progresses which include hidden data at intermediate blocks for data security and identity output. The comparison about special method algorithms is described below in *Table 3*. The Concept of Watermarking fingers-out that when noise is affected at the rate of 50% average value then it provides the authentic output. It also includes cropping process so that the noisy figure achieved less where noise is supplementary. This improvement gives resourceful result on discerning image.

Table 3 Comparison of Parameters for Various Algorithms of Steganography [1]

Method	Cover Image	Size of secret data	MSE	PSNR	Time (s)
MOD-10	Lena	18.1 KB	1.6301	50.23	8.63
	Baboon	18.7 KB	1.5802	51.61	8.52
IP	Lena	24.5 KB	0.2635	51.86	7.96
	Baboon	24.5 KB	0.2039	52.06	7.98
PVD 1	Lena	22 KB	12.471	37.87	8.6
	Baboon	25 KB	21.456	35.40	8.91
PVD 2	Lena	10.2 KB	8.4798	38.84	8.15
	Baboon	12 KB	7.4712	39.57	8.04
OPAP	Lena	25 KB	0.1503	56.71	7.56
	Baboon	25.8 KB	0.1620	55.96	7.66
DCT	Lena	100 B	0.0255	64.07	7.46
	Baboon	100 B	0.0244	65.15	7.38
Stream of 1's and 0's	Lena	21 KB	3.9013	42.21	8.77
	Baboon	21 KB	3.8091	42.33	8.456

The analysis is done on the 'Lena' and 'Baboon' images and it is clear that:

More size of secrete data
↓
Larger PSNR value
↓
Lesser Time dissipation
↓
Minimum Error

Here, the maximum achieved PSNR value is 65.1 dB.

Samer, Ammar and Putra **[15]**, show that both Watermarking and Steganography are two different techniques in terms of data to be communicated/ delivered. In case of Watermarking, the veiled data is having more protection and the cover image is concerned for the communication for the purpose of intellectual right protection. Whereas, in case of Steganography, the communicating object is the hidden data and its carrier is considered only as a medium of carrying this conceal information. Hence, we can say that therefore the copyright protection and preserving the intellectual rights, Watermarking is more suitable technique.

Emil, Hugues and Adam **[11]**, gathered the results for the image watermarking for robustness improvement using triangle meshes. The results obtained by them are as given below table 4 and 5. Table *4* describes the comparison of above four figures and highlights best result at the end.

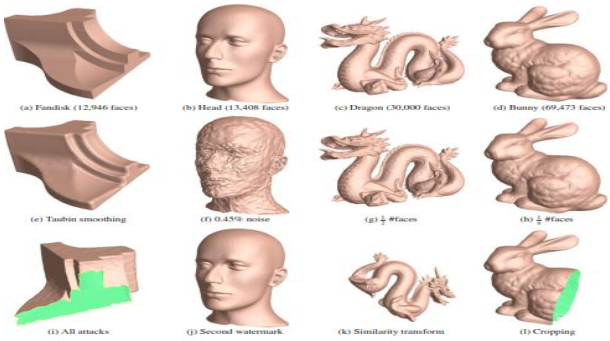

Fig 3: Watermarked Models with various Attacks [11]

Above figure 3 shows the different kinds of objects having different characteristics and they are tested against different attacks. The amount of errors produced is noted as in the table following:

Table 4 Typical Running Time in Minutes for Watermark Insertion and Extraction [11]

Stage	Fan-disk	Head	Dragon	Bunny
Conversion to PM	03	03	09	24
Water mark insertion	0.1	0.1	0.1	0.5
Registration	02	03	06	13
Resampling	15	15	45	120
Watermark Extension	0.2	0.2	0.8	02

The table following indicates the three basic techniques which performed the amount of noise and by which it's reduce. Generally, those techniques have ten powers few fraction Atto unit range but for noisy image it will increase and gives output with ten powers Pico unit range and this *snowballing* term indicates the expanse of noise. These credentials help to reduce the noise at precise matrix for a given image:

Table 5 Results of Three Basis Functions for different Attacks [11]

Model	Attack	Hat	Derby	Sombrero
Fan disk	Noise 0.2%	10^{-13}	**10^{-15}**	10^{-14}
	Noise 0.7%	10^{-02}	10^{-02}	**10^{-03}**
	Similarly Transform	10^{-17}	10^{-06}	**10^{-33}**
	Simplify ½ # faces	10^{-07}	10^{-05}	**10^{-12}**
Head	Noise 0.2%	**10^{-18}**	10^{-12}	10^{-12}
	Noise 0.7%	**10^{-05}**	10^{-03}	10^{-03}
	Similarly Transform	10^{-01}	10^{-03}	**10^{-24}**
	Simplify ½ # faces	10^{-02}	10^{-01}	**10^{-09}**

Consider the following table as the final analysis of this article:

Table 5 Final Comparative Analysis

Referred Technique	PSNR (dB) (Max.)	NC (NCC, SIM, SSIM) (Max.)
[14] Watermarking	42.8930	0.9889
[17] Watermarking	69.6876	1
[1] Steganography	65.1500	-
[18] Steganography	59.4200	-

The analysis of the above table indicates that for achieving better robustness and quality of data hidden for copyright and intellectual rights protection, *watermarking* is seen as more appropriate technique.

As it is very clear that cryptography technique do contain certain limitations and not suitable for intellectual rights' protection like copyright, ownership etc. after that the next generation named Steganography had been introduced and it is seen from the above comparisons that it provides a good level of data hiding and data security. Still it faces the challenges against detection of the data hidden by the statistical analysis. Also it is having the limitation towards robustness against the attacks like image rotation, resizing, lossy compression, noise etc. and also it depends upon the image format [15]. Therefore, as a special case of Steganography, Watermarking Technique is used. Thus it is seen as a sub division of steganography providing an evident tool for intellectual right protection and object ownership.

5. APPLICATIONS

The application areas of all three techniques for data hiding are given as below, in real time:

Table 6 Application Areas

Cryptography	Steganography	Watermarking
Credit Cards	Medical database systems	Medical applications
ATM Cards	Authentic communications in Armed Forces	Transactional watermarks (Fingerprinting)
Computer passwords	Access control systems	Owner identification
e-commerce	Terrorist attacks, to hide their identity	Intellectual rights protection
		Broadcast monitoring
		Copy control
		Covert communication

6. CONCLUSION

This article comes with conclusion that the two strategies- Steganography and Watermarking are the recent and *Efficient* Techniques for data Securities and Intellectual Rights Protection. Watermarking is a sub branch of the Steganography Techniques. In case of watermarking, most of the experiments are carried out for the *salt and pepper* and *compression* typed noises for robustness and fragility testing. For the fruitfulness of the research application for *Telemedicine*, Watermarking is chosen as more suitable method by analyzing the results obtained by the Research Scholars so far. In Telemedicine applications for the insertion of doctors' signatures and the patients' history onto the X-ray, MRI etc. images as per the properties of *watermarking*, it is considered as more suitable technique.

7. IMPLEMENTATION STRATEGY

As per the concluded results, Watermarking techniques are to be implemented for the Telemedicine application development as the future work of research. For the formation of the watermarks, from a number of transform domain techniques, the suitable and more appropriate technique is to be chosen because of its advantageous features against the conventional methods. This is then to be implemented as a next step of the research work done so far.

8. ACKNOWLEDGMENTS

For completion of this review paper successfully, we are thankful to all the scholars, guides and dear friends who directly or indirectly contributed to make our work done.

9. REFERENCES

[1] R. Amirathrajan, R. Akila, P. Deepikachowdavarapu, "A Comparative Analysis of Image Steganography", International Journal of Computer Application (IJCA), Vol. 2, Issue-3, pp.41-47, May 2010.

[2] A. Chaddad, J. Condell, K. Curran, P. MacKevitt, "A Comparative analysis of Staganographic Tools", University of Ulster, UK.

[3] J. Cummins, P. Diskin, S. Lau and R. Parlett, "Steganography and Digital Watermarking", the University of Bermingham, pp. 1-24, 2004.

[4] R. Popa, An Analysis of Steganography Techniques, The "Politehnica" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, http://ad.informatik.unifreiburg.de/mitarbeiter/will/dlib_bookmarks/digital-watermarking/popa/popa.pdf, 1998.

[5] A. J. Raphael and Dr. V. Sundaram, "Cryptography and Steganography- A Survey", IJCTA, Vol.2, Issue-3, pp. 626-630.

[6] John Wiley & Sons, Network Security, Bible, 2nd edition, "Communication Steganography compared to Cryptography", Safari books online, September 2009.

[7] D. Feng, W. Siu, and H. Zhang, Multimedia Information Retrieval and Management, 1st ed.: Springer, 2003.

[8] Jiang, X. "Digital watermarking and its application in image copyright protection", International Conference on Intelligent Computation Technology and Automation, ICICTA 2010, Changsha, China: IEEE Computer Society, May 2010.

[9] Chapter-13, Steganography and Watermarking, IV054, ppt.

[10] H. V. Desai, "Steganography, Cryptography, Watermarking: A Comparative Study", Journal of Global Research in Computer Science, Vol. 3, Issue-12, pp. 33-35, December- 2012.

[11] E. Praun, H. Hoppe and A. Finkelstein, "Robust Mesh Watermarking", Microsoft Research and Princeton University.

[12] G. C. Kessler, "Steganography: Hiding Data in Data", Windows and .Net magazine, April 2002.

[13] I. J. Cox, M. L. Miller and J. A. Bloom, "Watermarking applications and their properties", International Conference on Information Technology, CiteSeerXβ, Las Vegas, 2000.

[14] K. Pal, G. Ghosh and M. Bhattacharya, "A Novel Digital Image Watermarking Scheme for Data Security Using Bit Replacement and Majority Algorithm Technique", InTech, Watermarking, Vol. 1, May 2012.

[15] S. Atawneh, A. Almomani and P. Sumari, "Steganography in Digital Images: Common Approaches and Tools", IETE Technical Review, Vol. 30, Issue-4, Jul- Aug, 2013.

[16] P. Gupta, "Cryptography based digital iamge watermarking algorithm to increase security of watermark data", IJSER, Vol. 3, Issue-9, Sept 2012.

[17] H. Rawat, A. Kumar and S. Kumar, "Robust Digital Image Watermarking Scheme for Copyright Protection", IJCA, Vol. 75, Issue-18, Aug. 2013.

[18] S. Karve and V. Dalal, "Image Steganography using Inverse Embedding Reversible Data Hiding Scheme", International Conference and Workshop on Recent Trends and Technology, IJCA, 2012.