World of Computer Science and Information Technology Journal (WCSIT)
ISSN: 2221-0741
Vol. 4, No. 6, 68-75, 2014

Enhanced Wireless Transmitted Message Security By Encryption Complex Transformation

Dr. Oleg Viktorov
Middle East University, College of Information Technology,
Computer Information System Department
Amman, Jordan

Ahmed Shihab
Middle East University, College of Information Technology,
Computer Science Department
Amman, Jordan

Abstract -Wireless communications have less hacking immunity than wired communications. With the increase of dependability on wireless data transfer and calling, it is necessary to develop new rigid algorithm to add more levels of security on the wireless data. In the fact, the effort that is continuously put in hacking the wireless transmitted data is more than the effort that is put in building secure communication channels. A packet transfer security model for wireless communication by the mean of cryptography and complex transformation. Was presented a secret key encryption / decryption algorithm was developed and presented in this paper. The encryption algorithm is demonstrated to decrypt the message and convert it to meaningless rapish data. The cryptographic encryption / decryption of the wireless packet is a first level security procedure, while the second level of security is being added by sending not the encrypted packet itself, but the complex transformation of that packet. Discrete cosine transform (DCT) and discrete wavelet transform (DWT) have been compared. The comparison was bases on peak signal to noise ration (PSNR) and mean square error (MSE). The wavelet transformation space is larger than the discrete cosine transform, so, the PSNR was much higher in DWT than DCT. The MSE is approximately the same for both.

Keywords – wireless security; encryption; discrete wavelet transform; discrete cosine transform.

I. INTRODUCTION

Secrecy of information is being considered as a high priority issue since the ancient world. The information that contains messages has two cases of secrecy weaknesses; storage or saving of the message, and message transfer. From the ancient world, human was faced a big deal to hide the transferred message from source to destination [1].

The rise of the modern technology increases the problem of data security and enlarges the problem of hiding the message data in old methodologies. In fact, the paper messages become rare in the age of cellular communications and Internet technology. This state triggers the modern computer scientists to conduct researches in encryption / decryption and data security. Hiding the message contents in effective way in order to achieve a rigid secure message transfer is very important issue wireless transfer has less immunity than the wired communications.

In modern computer transfer technology, the cryptography is the most known science that is used to hide data in order to add a level of security to it. Many encryption and decryption algorithms are implemented to change the shape of the data in order to hide its contents [1].

Actually, the message after it encrypted by a cryptography technique will be a rapish data and it not represents the actual message context in human or computer perception. In computer digital world, the cryptography was adapted by the means of encryption / decryption of information while transferring it and storing.

In modern years, the computer technology added more complexity and flexibility in data communication than any time ever. The messages become very easy to be transported. The cryptography has to be adapted and improved in terms of data encryption and compression. Moreover, the encrypted message is clear, the line inspector could know that, there is a message here, but he couldn't understand it, or he is not able to derive a reading methodology for it. If the message itself was fetched, so, it is hard to break it. While the contexts of the message is encrypted, no interference between different types of messages, also, no ease hacking is possible and thus the protection and isolation of the message both are goals of the encryption of the message [8] [5].

Hiding information – especially in communications - has a large scale variety and importance. Many centuries across, hiding information was used in different traditional techniques. In the modern world, the secret message hiding becomes more important, more critical, and more difficult. Another issue that faces all people those is used to send critical messages over transport layer over internet. The internet service provider (ISP) in many cases does not offer a reliable secure internet service even in browsing. The dependency on Internet becomes very risky. So, if users depend on the Internet to send secure messaging directly, the transfer of critical messages will be very risky [1].

Critical packets could fall in two categories; the first is secret contents messages which is used by security directorates and departments in the most cases, also, it is being used by the companies and institutions to keep the secret data confidentiality The second type is the priority messages which is not really required to be secret, but it is must to reach the destination from the source without any change. While a very few change in that transferred message could cause a big deal. The first type of messages is hardly required to be secret and confidential. The confidentiality of those messages is much important than the reliability of the transfer itself. This means that, even though the transfer may face much failure, it should be at top secrecy level to keep secret and no one can reach its contents. Whereas, the second messages type is the category of messages that includes automatic commanding of physical system or computer system, or even contains a commercial data; including the messages that contains a type of data that affects the decision making process of the computerized system. This type of messages are a combination of the two critical messages categories; it is required to be secret to prevent any intrusion from hacking or affecting the decision making process in any circumstances. Also, it is top priority to make reliable transfer that could be in real time in many cases [1] [5] [8].

In recent years the techniques that are used in the decryption evolved significantly. So the cryptography science considered one of the most hot computer science topics that attempt to get a high level of data protection. Cryptography is a way to hide the secret information. By theory, it aims to protect the information for counter attack. The presence of hidden information in the digital word is concerns of protecting the data from attack while transfer over internet or any other equivalent communication media (i.e. mobile cellular GSM phones). Modern researchers were focusing on developing different techniques in order implement and met the requirements of different aspects that could handle the secret message transfer. Furthermore, some issues should be handled and criteria could be achieved. The criteria include the security level at first, and also including message size, variance and immunity against noise. The big deal in cryptography is that, the security of the message, most techniques that was developed overcomes low security due to direct encryption of the sent message. Direct encryption means that, the transmitter terminal uses a common encryption algorithm either it is a public key or secret key. These techniques in the emerging technology of the cryptography and computerized statistical analysis, becomes a type of possible to be broken in a trails of statistical logging programs. So, the level of security that uses direct encryption becomes weak in a way that the logging programs could achieve many trials on it to get the consistency in that context. Once the consistency is got, the message becomes easy to be broken, and the contents will be interpreted quickly [1] [4].

A reliable secure transfer should be based in high level of secure encryption in order to hide the context of the message that is subjected to be sent, with cooperation of another complex methodology that adds a high security fixture as a second level of complexity.

This paper is presenting a high level of secure adaptive algorithm to enable transfer a secret data over wireless communication media. The data is intended to have high security by contributing mathematical based cryptographic encryption of the sent message and decryption of the received one as the first level of security. Thus, the message context will be hidden. Another level of security will be adopted by the mean of mathematical complex transformation. So, the encrypted message will be transformed mathematically before sending via wireless media. Two transformations will be used separately, and this paper will include a comparison between them with respect signal to noise ration, and mean square error. They are discrete cosine transform (DCT) and discrete wavelet transforms (DWT) [3] [7].

II. TRANSFORMATION

The process of feature extraction aims to extract a set of essential characteristics that can identify or represent whole of specific signal. Hence the text message could be represented as a two dimensional signal, so, it contains many unique characteristics that are specific for each individual, and contain information that allow to make a complex mathematical operations on it. Different methods could be used to process as context of data as a signal; Discrete Fourier Transforms (DFTs), Discrete Cosine Transform (DCT), Laplace Transform, Discrete Wavelet Transform (DWT), etc ψ [6].

Wavelet Transform provides a useful decomposition of a signal, so that faint temporal structure can be revealed and handled by nonparametric models. With wavelets, it is possible to analyze a signal at several levels of resolution, making it possible to capture transient, high-frequency bursts with poor frequency resolution and also slowly varying characteristics with high-frequency resolution. Therefore, it is possible to trade off between frequency resolution for better time resolution (for analyzing transients) and time resolution (for analyzing slow variations). A facility is not afforded by the short-time Fourier transform [3].

As it well known, the digital signal processing (DSP) is computer based mathematics that operates with special type of data signals. These signals are obtained from different sensors, like microphone or camera. DSP is mixed mathematics and algorithms that are used to manipulate the signals, which are converted to the digital form signals. Two types of digital signal parameter categories are exist: independent (usually it is time) and dependent variables, which represent what are measured. If these parameters are belonging to the continuous range of values, it is called continuous signal. When the continuous signal pass through Analog- to- Digital Converter (ADC) it said to be discrete or digitized signal. The digital signal can contain frequency component only up to one half of the sampling rate. Generally, continuous signal are natural signal, while discrete signal exist mostly inside the computers. A signal that uses frequency as the independent parameter are said to be frequency domain represented signal (i.e. transforming the signal to frequency domain using Fourier transformation, wavelet transformation, discrete cosine or discrete sine transformation, etc) while signals that use time as independent parameter are said to be in the time domain. Transform of a signal is just another form of representing it in different domain the default one, which is the time domain. It should not change the information content present in the signal [2].

Wavelet transform is a technique for analyzing the signals that developed to overcome the problems related to its frequency and time resolution, more specifically it provides uniform time-resolution for all frequency. Wavelet analysis allows the use of long time intervals where more precise low-frequency and shorter regions where high frequency information needed. Wavelet transformation is either continuous or discrete [2].

The continuous wavelet transform (CWT) is defined as the sum of over all time of signal multiplied by scaled, shifted versions of the wavelet function. The results of (CWT) are set of Wavelet coefficients, which are a function scale and position. Dilation and translation of the Mother function, or analyzing wavelet Φ(x) defines an orthogonal basis, as shown in equation (1) [10]

$$\Phi_{(s,l)}(x) = 2^{\frac{-s}{2}}\Phi(2^{-s}x - l) \qquad \text{............ (1)}$$

The variables s and l are integers that scale and dilate the mother function Φ(x) to generate wavelets, such as a Daubechies wavelet family. The scale index s indicates the wavelet's width, and the location index l gives its position. The mother functions are rescaled, or "dilated" by powers of two, and translated by integers. What makes wavelet bases especially interesting is the self-similarity caused by the scales and dilations. To span the data domain at different resolutions, analyzing wavelet is used in a scaling equation (2) [10]:

$$W(x) = \sum_{k=-1}^{N-2}(-1)^k C_{k+1}\Phi(2x+k) \qquad (2)$$

Where W(x) is the scaling function for the mother function and Ck are the wavelet coefficients. The wavelet coefficients must satisfy linear and quadratic constraints of the form (3) [10]:

$$\sum_{k=0}^{N-1} C_k = 2, \quad \sum_{k=0}^{N-1} C_k C_{k+2l} = 2\delta_{l,o} \qquad (3)$$

The decomposition process can be iterated with successive approximate so that the one signal is broken down into many lower resolution components this is called the wavelet decomposition tree. Figure (1) illustrates the decomposition (DWT) coefficient. Since the analysis process is iterative, in theory it can be continued indefinitely. In reality, the decomposition can proceed only until the individual details consist of a signal sample [3].

Where low pass filter removes all frequencies that are above half of the highest frequency in the signal. Several families of wavelet like Harr, Daubechies, coiflets, symlets, meyer, Morlet, Mexican Hat, etc could be adapted to be applied in text message complex transformation. Figure (2), illustrates several different wavelet families [3].

Daubechies wavelet is the most popular wavelet transformation family. It is a family of orthogonal wavelets defining a DCT and characterized by a maximal number of vanishing moments for some given support. With each wavelet type of this class, there is a scaling function (also called father wavelet) which generates an orthogonal multi-resolution analysis. They represent the foundation of wavelet signal processing and are used in numerous applications [5].

The Harr, Daubechies, Symlets and Coiflets are compactly supported the orthogonal wavelet, where Coiflets wavelets are more symmetric vanishing moments than Daubecheis wavelet. This paper uses Daubacheis wavelet family in order to make an honest judge in the comparison of wavelet transformation with discrete cosine transformation results [3].

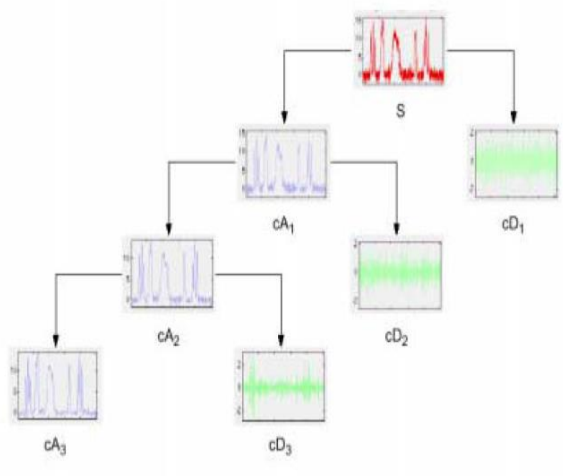

Figure 1. Decomposition (DWT) coefficients.

The discrete cosine transform (DCT) is another technique for converting a signal into elementary frequency components rather than the wavelet transformation methodology. It is widely used in signal security, image compression, signal immunity, and others. The functions that computes the DCT is a mathematically powerful functions [12].

In general, transformation coding constitutes an integral component of contemporary messages processing applications. Transform coding relies on the premise that bits in a digital stream exhibit a certain level of correlation with the other stream bits. In text messages, the pixels show a high correlation. Consequently, these correlations can be exploited to predict the value of a character from its respective line of text. A transformation is, therefore, defined to map this spatial (correlated) data into transformed (uncorrelated) coefficients. Clearly, the transformation should utilize the fact that the information content of an individual pixel is relatively small.

The discrete cosine transform (DCT) is another technique for converting a signal into elementary frequency components rather than the wavelet transformation methodology. It is widely used in signal security, image compression, signal immunity, and others. The functions that computes the DCT is a mathematically powerful functions [12].

In general, transformation coding constitutes an integral component of contemporary messages processing applications. Transform coding relies on the premise that bits in a digital stream exhibit a certain level of correlation with the other stream bits. In text messages, the pixels show a high correlation. Consequently, these correlations can be exploited to predict the value of a character from its respective line of text. A transformation is, therefore, defined to map this spatial (correlated) data into transformed (uncorrelated) coefficients. Clearly, the transformation should utilize the fact that the information content of an individual pixel is relatively small.

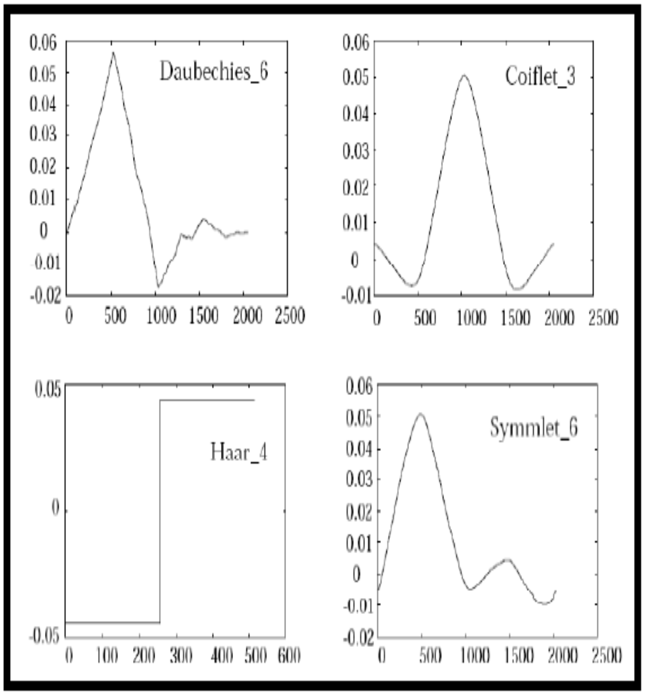

Figure 2. Different wavelet families

Therefore, DCTs are used to convert data into the summation of a series of cosine waves oscillating at different frequencies (more on this later). They are very similar to Fourier Transforms, but DCT involves the use of just Cosine functions and real coefficients, whereas Fourier Transformations make use of both Sins and Cosines and require the use of complex numbers. DCTs are simpler to calculate. Both Fourier and DCT convert data from a spatial-domain into a frequency-domain and their respective inverse functions convert things back the other way [12].

The discrete cosine transform are used extensively in multimedia to compress analog signals, often it discards information, to enable efficient compaction. It is important to be careful about what information in a signal could be discarded when removing bits to compress a signal. DCT helps with this process.

The human eyes, ears and perception are analog devices and they are less sensitive to distortion around edges, also, they are less likely to notice subtle differences fine textures. The cosine transformation uses the similarity and consistency between the elements of the signal stream. If the signal pattern was not affected by removing the higher frequency elements of their context, so, it is possible to change the domain of the signal pattern and return back to its original domain with a negligible measurable change.

DCT is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry. The obvious distinction between a DCT and a DFT is that the former uses only cosine functions, while the latter uses both cosines and sins in the form of complex exponentials.

The DCT in comparison with DFT has two main advantages; it's a real transform with better computational efficiency than DFT which by definition is a complex transform. And, it does not introduce discontinuity while imposing periodicity in the time signal. In DFT, as the time signal is truncated and assumed periodic, discontinuity is introduced in time domain and some corresponding artifacts are introduced in frequency domain. But as even symmetry is assumed while truncating the time signal, no discontinuity and related artifacts are introduced in DCT. So, the discrete cosine transform could evaluate the lines better than the discrete Fourier transform, thus, it is better to work with DCT for linearity purposes. Figure 3 shows the result of line estimation using both, DCT and DFT [11].

As any mathematical transform, the discrete cosine transform could be implemented for single dimensional signal, two dimensional signals, or any other multi-dimensional signal. Equation (4) shows the general form of one dimensional discrete cosine transform. And the inverse cosine transform is shown in equation (5) [11].

$$C(u) = \alpha(u)\sum_{x=0}^{N-1} f(x)\cos\left[\frac{\pi(2x+1)u}{2N}\right] \quad (4)$$

$$f(x) = \sum_{u=0}^{N-1} \alpha(u)C(u)\cos\left[\frac{\pi(2x+1)u}{2N}\right] \quad (5)$$

for u = 0,1,2, , … N-1
And α(u) is defined as

$$\alpha(u) = \begin{cases} \sqrt{\frac{1}{N}} & for \quad u = 0 \\ \sqrt{\frac{2}{N}} & for \quad u \neq 0. \end{cases}$$

In the same way, the general form of the two dimensional discrete cosine transform is shown in equation (6). The 2-D basis functions can be generated by multiplying the horizontally oriented one dimensional basis function in equation (4) with vertically oriented equivalent function. It can be noted that the basic functions exhibit a progressive increase in frequency both in the vertical and horizontal direction [1].

$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y) * \cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (6)$$

for u = 0,1,2, … N – 1
v = 0,1,2, … N – 1

Where the inverse discrete cosine transform in two dimensional forms is gotten by the equation (7).

$$f(x,y) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} \alpha(u)\alpha(v)C(u,v) * \cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (7)$$

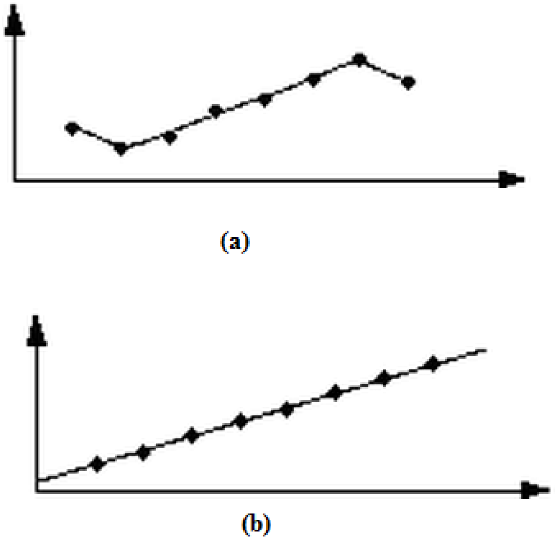

Figure 3. Line estimation using DFT (a) and DCT (b)

This paper purpose is to use the discrete wavelet transformation and discrete cosine transformation to add a second level security on the message that transferred by any wireless media. A comparison will be shown in the result section between both; discrete wavelet transforms (DWT) and discrete cosine transform (DCT) with respect to applied signal. The assumption is that, the message is a two dimensional signal, because of that, any data that is subjected to be sent via wireless media is easily could be represented as a two dimensional form of encrypted data, that if its origin is not two dimensions [11].

The transformation is will be done on the encrypted data, so, no any further processing will be used to represent the transformed signal.

III. METHODOLOGY

In the time of Internet, cellular communication, and all types of wireless transfer, the computer era becomes the motivated engine to all security researchers. This paper implements a two level of security cryptography system based on complex transformations in order to create a high level of security to the transferred data via wireless communication.

The system that presented in this paper consists of two levels in order to send a secure message. The secure message that could be sent is either text or image. The result for both, text messages and images will be demonstrated in the "Results" section. Figure 4 shows the block diagram for the encryption part the implemented system. The receiver terminal part is shown in Figure 5. This terminal is the part that interprets the received encrypted message and retrieves the original send message.

The message initially will be held in the sender space. It will be encrypted mathematically in the first operation. The encryption will hide the message and replace it with rapish data that is encrypted using secret keying. The encryption will done mathematically be replacing the meaning full message by another encoded one that contains no any understandable information.

Equation (8) presents the encryption of each single element of the message signal. The element of the message signal could be a character if it is a text message or a pixel value if it is an image.

Ei,j = Ci,j + (max(Ms)) –(min(Ms)) * (j + i) .... (8)

Where

Ei,j: is the encrypted message element;
Ci,j: is the original message element;
Ms: is the total message;
i,j : is the message element index in the row and column.

CRC is being added to the end of each encrypted message in order to ensure the validity of the received data with respect to receiver terminal.

The encryption represents the first level of transfer security, whereas, this level add just a few security scope, because of that, many programs that log into the received data via wireless protocol uses statistical calculation and trials to detect the consistency inside the received signal. This statistics based programs do a large number of calculations and trials which in most cases capable to detect the consistency of the signal. Once the consistency is detected, the message becomes easy to break. So, this paper didn't depend on the encryption to add a high level of security, but is very helpful security level with the aid of complex transformation.

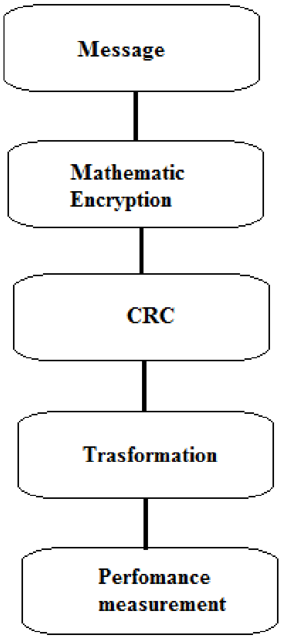

Figure 4. Block diagram for the processing at the sender terminal

It is not realistic to transmit critical data via wireless media directly after transforming it using any transform. Because of that, the intrusion will try the whole known transforms, and it will get the message breached. So, in order to do the security reliable and efficient, the message signal could be transformed into a complex domain after it encrypted using the presented encryption algorithm in this section.

The encrypted message could be transformed to complex domain via either discrete cosine transform (DCT) or by discrete wavelet transform (DWT) in this paper. The DCT and DWT methodologies and theories are illustrated in section 2. This paper presents two modules; the first module uses DCT while the second uses DWT. The aim of this paper is to compare the presented two algorithms and recorded the results.

The receiver terminal will apply these concepts in reverse way in order to extract the real text message from the received encrypted one. Once the message is being received decryption procedure will extract the meaningful message after computing the inverse transformation of that received message. The receiver signal will decrypt the message by the meaning of secret keying cryptography.

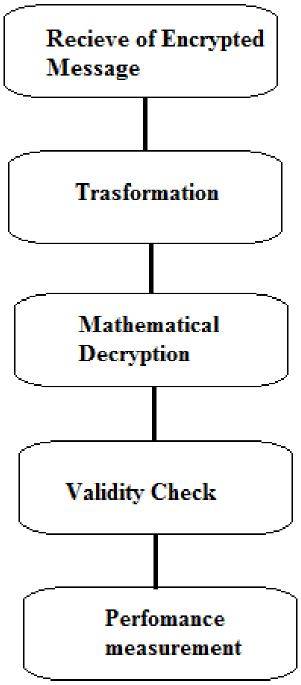

Figure 5. Block diagram for the processing at the receiver terminal

IV. RESULTS

Security measurement is designed to measure and analyze digital packet that represents the transmitted data. In this paper, two security measurements were used; peak signal to noise ratio (PSNR), and mean square error (MSE). These measurements were applied to the encrypted and decrypted message to investigate the effect of the contributed algorithmic technique on the packet. It measures considered the standard metrics to evaluate the security level.

The mean square error (MSE) is being calculated using equation (9), while the peak signal to noise ratio is being calculated using equation (10). Where "MAXi" is the maximum.

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \qquad (9)$$

$$PSNR = 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE) \qquad (10)$$

A total test sample around 90 packets was used to test the presented algorithm and to test the result. Each packet where encrypted, transformed to both, discrete wavelet transform and discrete cosine transform separately, and sent to the other terminal by simulation of the wireless transfer media.

On the receiver terminal, the simulation of wireless transfer receives the sent packet, inversely transform it to the original time domain, and decrypt it. The results was recorded for the whole set of data. The approximately 90 samples of packets were selected to be a various set of different data contents, different data size, and different types of context. This differences enables to correctly measures the precision of the measurement.

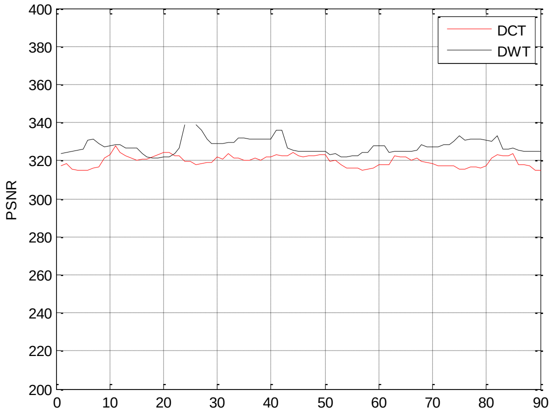

Figure 6. PSNR of the transferred packets

Figure 6 shows the packets peak signal to noise ratio for the data set, the largest PSNR means more rigid algorithm and more noise immunity. Figure 6 shows that, the higher PSNR was gotten using discrete wavelet transformation (DWT). In fact, the discrete cosine transform (DCT) has some noise immunity but is much less than DWT.

Figure 7 illustrates the mean square error (MSE) between the transmitted packet and the received one. The result of both DCT and DWT are similar, and the result is approximately the same

Table1 below illustrates the strength of the presented algorithm against two different statistical logging programs, the programs are applied to transmitted packed in order to try to break it.

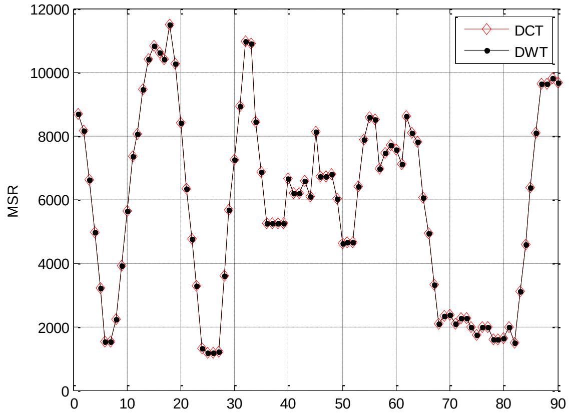

Figure 7. MSE of the transferred packets

TABLE-1: RESULT OF APPLYING HACKING PROGRAMS TO THE PRESENTED ALGORITHM

Hacking program	Weakness result
Frequency domain analysis	11%
Time domain analysis	9%

V. 5. CONCLUSION

The wireless security is not an easy task in the rapid rise of the computer technologies and the advances in statistical logging programs. Traditional cryptography algorithms becomes un able to efficiently ensure security transfer of data packets in wireless communication. So, the concepts of digital signal processing (DSP) could be implemented in a way to ensure complex cryptography that hides the data in a way that meets two criteria; low signal distortion and high security level.

A high security wireless data packet transfer via two level security paths is presented in the paper the first level is mathematical encryption of the packet, while the second is transform the encrypted packet to different signal domain. Two transforms are demonstrated in this paper: discrete cosine transform (DCT) and discrete wavelet transform (DWT).It is hard to break security layer on the transmitted packet using the complex transformation.

REFERENCES

[1] Ross, John. “The Book of Wireless: A Painless Guide to Wi-Fi and Broadband Wireless”, Second Edition. San Francisco, 2008.

[2] Dr. H. B. Kekre, Archana B. Patankar and Dipali Koshti, “Performance Comparison of Simple Orthogonal Transforms and Wavelet Transforms for Image Steganography”, International Journal of Computer Applications (0975 – 8887) Volume 44 No 6, April 2012.

[3] I. V. Oseledets, E. E. Tyrtyshnikov. “Algebraic wavelet transform via quantic tensor train decomposition” SIAM J. Sci. Compute. V. 33, No. 3. PP. 1315-1328. DOI: 10.1137/100811647. 2, 7, 8, 2011.

[4] Sherin Youssef, Ahmed Abu Elfarag, Reta Raouf, “A Robust Steganography Model using Wavelet-based Block-partition Modification” /International Journal of Computer Science &

Information Technology/ (IJCSIT) pp. 15-28 Vol 3, No 4, August 2011.

[5] Ali Al-Ataby and Fawzi Al-Naima, “A Modified High Capacity Image Steganography Technique Based on Wavelet Transform”, The International Arab Journal of Information Technology, pp. 358-364 Vol. 7, No 4, October 2010.

[6] T. von Petersdor, Ch. Schwab. “Wavelet Discretization’s of Parabolic Integro-differential Equations” SIAM Journal on Numerical Analysis. 2003. V. 41, No 1. PP. 159–180. DOI: 10.1137/S0036142901394844.

[7] Dr. H. B. Kekre, Tanuja K. Sarode, Sudeep D. Thepade, Ms.SonalShroff, “Instigation of Orthogonal Wavelet Transforms using Walsh, Cosine, Hartley, Kekre Transforms and their use in Image Compression” /International Journal of Computer Science and Information Security/ Volume 9, No 6, pp. 125-133, 2011.

[8] Dr. H. B. Kekre, Ms. Archana Athawale, “Information Hiding using LSB Technique with Increased Capacity” /International Journal of Cryptography and Security/ Vol I, No 2, Oct.2008.

[9] I. W. Selesnick. “Wavelet transform with tunable Q-factor”. IEEE Trans. Signal Processing, 59(8) PP.3560–3575, August 2009.

[10] I. Bayram and I. W. Selesnick. “Overcomplete discrete wavelet transforms with rational dilation factors”/ IEEE Trans. Signal Processing/ 57(1):131–145, January 2009.

[11] H. Olkkonen, J. T. Olkkonen, and P. Pesola. “FFT-Based computation of shift invariant analytic wavelet transform”/ IEEE Signal Processing Letters/ 14(3)PP.177–180, 2007.

[12] N. J. August and D. S. Ha , “Low power design of DCT and IDCT for low bit rate video codecs,” IEEE Transactions on Multimedia, Vol. 6, No 3, pp. 414–422, June 2004.