جامعة نايف العربية للعلوم الأمنية
Naif Arab University for Security Sciences

Naif Arab University for Security Sciences
Journal of Information Security & Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

Enhancing PC Data Security via Combining RSA Cryptography and Video Based Steganography

Nouf A. Al-Juaid [1*], Adnan A. Gutub [2], Esam A. Khan [3]

[1] *Department of Computer Science, College of Computing and Information Technology, Shaqra University, Shaqra, Saudi Arabia.*
[2] *Computer Engineering Department, College of Computers & Information Systems, Umm Al-Qura University, Makkah, Saudi Arabia.*
[3] *The Custodian of the Two Holy Mosques Institute for Hajj & Umrah Research, Umm Al-Qura University, Makkah, Saudi Arabia.*

Received 04 Jan. 2018; Accepted 15 Mar. 2018; Available Online 17 Apr. 2018

Abstract

This paper proposed an enhanced system for securing sensitive text-data on personal computer benefitting from the combination of both techniques: cryptography and steganography. The system security is generated by involving RSA cryptography followed by video based steganography as two sequential layers to insure best possible security gaining the advantages from both. The study modeled the system and implemented it to be tested to explore the relation between security, capacity and data dependency. The experimentations covered testing securing data within 15 different size videos showing interesting results. The research gave enhancement to capacity vs. security, as enforced unavoidable tradeoff. The work uniqueness is presented in showing different measures allowing the user and application to be the decision maker to choose. The tests provided all possibilities of accepting security of 1-LSB, 2-LSB, and 3-LSB methods detailing their effects on the cover video. The main outcome proved applicability to be adopting 3-LSB approach to give acceptable security with practical capacity preferred making 3-LSB winning among 1-LSB and 2-LSB techniques.

I. Introduction

Usually, we need to secure sensitive data that we store on personal computers such as e-mail messages, health information, family private pictures, bank information, and credit card information. Securing sensitive secret text in the personal computers (PC) has benefit of the capability to allow the PC available files to act as the private cover [1]. In order to provide confidence and safety to the user to protect his information on a PC, we combine cryptography and steganography techniques, i.e. for hiding sensitive data, as presented earlier for hiding in images [2] but here utilizing video based steganography. The security obtained using steganography to conceal sensitive data inside a cover media depends on the belief that no one can suspect that there is any data hidden. However, if anyone notices that there is a change in the cover media, the sensitive data can be discovered [3]. Therefore, it is preferred to use another technique such as cryptography to encrypt the sensitive data before hiding it in the cover media. That will ensure that even if the embedded text is discovered, no one can know its content because it is encrypted [4]. Therefore, for higher security, we can take advantage of combining the two techniques to ensure that even for the very difficult security penetration; still the

Keywords: *Securing text on PC, RSA cryptography, Video based steganography, user preference security, merging cryptography and steganography*

Production and hosting by NAUSS

* Corresponding Author: Nouf A. Al-Juaid
Email: naljuaid@su.edu.sa

doi: 10.26735/16587790.2018.006

sensitive data are not harmed or used negatively. This research paper presents a 2-layer crypto-stego security system utilizing video base steganography as PC dependent layer as well as RSA cryptography as independent assurance layer.

Steganography in general, is the science of concealing information through a certain process in another cover medium type, i.e. text, image, audio and videos [2]. This work focuses on video based steganography where the imbedding is performed with the encrypted secret hidden in the cover object [3]. Cryptography, as the other layer within this security system, is mainly encrypting the secret plain text converting it to cipher text [1]. In our security system, the sensitive text data passes through the crypto layer followed by the steganography layer resulting the output file as stego-video. Fig. 1 shows the main overview of the method using this two-layer techniques.

In this work, we suggested and implemented the flexible two layers technique, i.e. cryptography and steganography, to benefit from both and give the best possible security dedicated for PC applications. The cryptography layer is using RSA crypto algorithm assuming its security reputation and simplicity[5].The steganography layer is adopting the video based steganography due to its popular availability and personal favor in PCs[1]. This video based steganography is concealing the ciphered text in the least significant bit (LSB) [6]and trying to improve its capacity by increasing the number of hiding LSBs, similar to the principle idea in [7].

The structure of this paper is as follows. The following section, Section 2, presents brief literature review of related work and similar ideas that should be considered in this study. This related work section is describing several techniques using video steganography with cryptography to secure data, which all found appropriate for PC data securing. Section 3 shows our suggested crypto-stego security system design, pursued by a short explanation of the implementation and simulation in Section 4. Section 5 focuson the relation of system security, capacity and data dependency. The section experiments are stressing on the benefit of changing the stego number of LSB used affecting the security system running the program on 15 different videos observing attractive comparison results. Finally, in Section 6 concludes the paper with the giving possibilities and plans of future work.

II. Literature Review

Many techniques are found in the literature appropriate for PC security applications. This section reviews research that integrated the two techniques of cryptography and steganography utilizing video covers. Deshmukh et al.[8] introduced a hash-based LSB method for video steganography that conceals secret data or information within a video. Firstly, the location of the insertion in the LSB bit is determined using a hash function. Then, the secret text is concealed in the selected position of the LSB. In this paper, they applied the method to AVI files

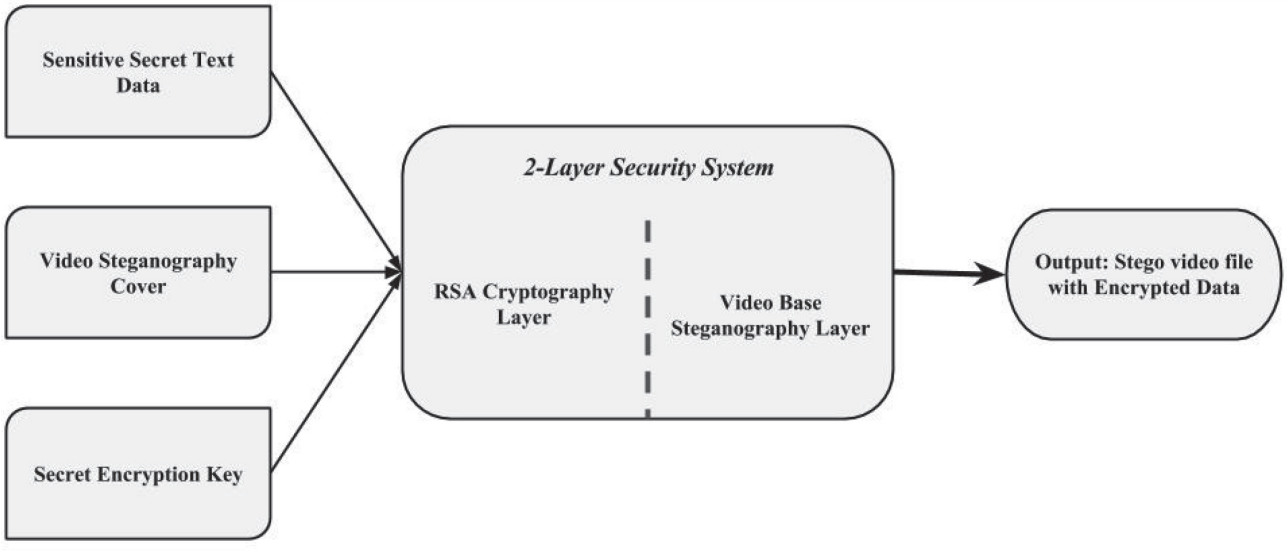


Fig. 1. Overview of the proposed 2-layer security system.

and measured the PSNR and MSE for comparison with the original video file.

In contrast, Singh in [9] suggested a way to embed text in video files using LSB substitution. The embedding is done in a location in LSB bits according to equations noted in the paper. The advantage of this method is a simple and successful process for hiding secret messages more securely.

Gupta and Chaturved in [10] proposed an approach to conceal hidden text into a video file in two steps. The text is ciphered using an AES algorithm and then inserted into a video file using LSB substitution. The approach was applied to video frames in 1 LSB, 2 LSBs, and 3 LSBs of each pixel. They compared the results using the PSNR correlation factor and found that when three LSBs were used and an AES algorithm , the security was increased.

A different approach to conceal text in a video file was discussed by Prabhakaran et al. in [11]. They implemented a system combining cryptography and video steganography in two layers. In the first layer, i.e., the cryptography layer, the confidential data are encrypted using an AES algorithm. In the steganography layer, the sensitive data are concealed in a video cover using a motion vector. The advantage of this approach is that the hidden data do not distort the video file, hence keeping the quality of the video acceptable.

In addition, Aly [12] proposed a method to hide the data using the same technique as in [16], using motion vectors on MPEG-2 compressed video. The findings of this research were measured according to two parameters: video quality and data size. This work showed that even with increased data size, the distortion of the video quality is low.

Another method using many-covers audio and video was presented in [13] by Praveen et al. They implemented a method that combines cryptography with audio and video steganography, with the intent of concealing text and images simultaneously inside the audio–video file. They suggested encrypting text and images using an advanced chaotic technique. They then inserted the encrypted image inside video frames using 4 LSBs and embedded the encrypted text inside an audio file using the LSB.

In addition, a technique using LSB insertion into a video file to hide secret text was proposed by Swathi et al. [14]. A data-hiding technique embeds the information based on the stego key generated from polynomial equations.

Moon and Raut in [15] introduced a method to enhance security in video steganography. They used 4 LSBs substitution to conceal an enormous amount of data in a video in specific frames. It is hard to find in which parts of the video the text is embedded, and the security is increased because a human observer cannot detect the data is hidden.

A last work related technique for concealing encrypted secret message inside a cover file has been presented by Bodhak et al. [16] improved video steganography by designing a method to embed the text file in a video file differently by utilizing DCT and LSB. The advantage of this system is that data is hidden highly securely and consistently in AVI videos.

All the above methods have been investigated and well thought-out to propose our enhanced data security 2-layer system for securing sensitive text data appropriate for personal computers. Our method combines cryptography and steganography as two independent sequential layers with all their security features. The system added more studies relating the steganography layer to the PC videos bits and the secret sensitive text data bits. Next sections will present the design and implementation of our system and its comparisons in more depth.

III. Proposed System Design

To ensure high security appropriate for PC applications, advantaging from the many techniques presented in Section 2 above, our suggested system using both cryptography and steganography. In fact, cryptography and steganography are both exploited as separate layers to give the best possible security with independent security, capacity, and reliability measures and improvement adjustments.

The flexible system can be observed as a process flow graph Fig. 2 clarifying the storing point of view as well as the retrieving point of view.The cryptography layer is using RSA crypto algorithm, is a public cryptographic system that depends on two keys: one for encryption and the other for decryption. The RSA algorithm solves the problem of key management and key distribution [17]. It can be understood in more depth in many resources such as [18].

The steganography layer in our system is using the video based steganography as in hiding the ciphered text coming out of the cryptography layer. In fact, we improved the system capacity trying to increase the hidden bits in the video using several least significant bits (LSBs) instead of only one.

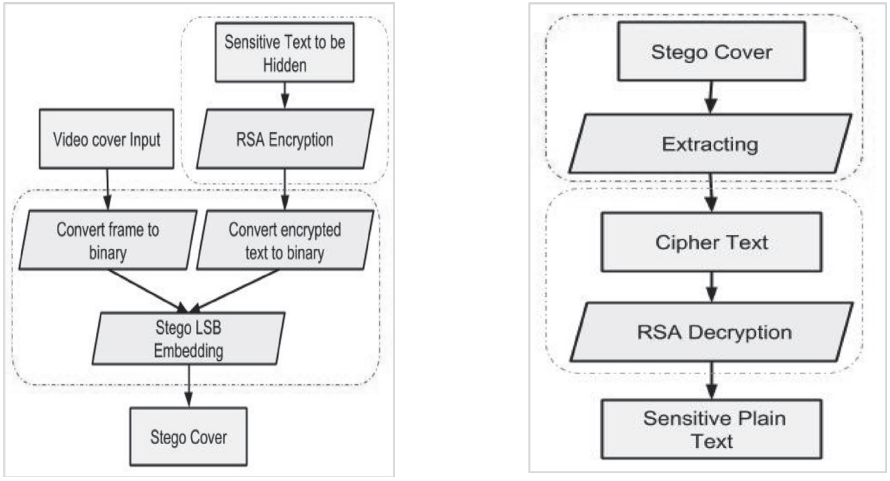


Fig. 2. Process flow graph of the proposed 2-Layer security system

IV. The Security System Implementation

This proposed high security system for sensitive PC data has been designed and implemented in a research MATLAB platform. The MATLAB programming language is chosen because it offers high-performance numerical computation, data analysis, visualization capabilities, and application development tools [4]. In addition, MATLAB functions are easy to use; a user interface function guides the user through the process of either encoding or decoding a message into or from the image, respectively. MATLAB provides the ability to call external libraries, such as Open CV and instant access to thousands of essential and specialty functions written by experts. MATLAB has a large user community with lots of free code and knowledge sharing. Another attractive feature found in our MATLAB software platform is clearly written documentation with many examples. The aim of this implementation is to study and elaborate the 2-layer security system idea in depth as well as to test different situations to enhance this important academic research field. The implementation is putting a target of helping security crypto designers and programmers to improve our system idea and make it practically usable.

Running the system implementation begins with the user enter the secret sensitive text data message and the secret key, which is representing starting the operation of the crypto layer. Within this layer process, the program converts each character of the sensitive secret text into an array of binary bytes to be encrypted using RSA. The second layer, i.e. steganography layer, also asks for an RGB video frame as cover media, such that its pixels are also converted into binary form. This stego layer can start its process at the same time while crypto layer is running, i.e. preparing the video frame as binary bits, but cannot start hiding data except after ciphertext is generated from the crypto layer. Any pixel on the RGB video frame has 3 channels, namely red, green and blue (RGB) shows a byte of 8 bits each. Therefore, using the least significant bits (LSB) video based steganography in our original system, we could conceal in each pixel 3 bits of secret data.

The implementation of the proposed method interface can be observed in Fig. 3. The system testing used the stego cover as a video cover of 141 frames of 240x320 pixels as the size of the frame. The implementation example uses the fixed secret text data message Text with almost 600 characters and 101 words as follows: ‘Most people who bother with the matter at all would admit that the English language is in a bad way, but it is generally assumed that we cannot by conscious action do anything about it. Our civilization is decadent and our language so the argument runs must inevitably share in the general collapse. It follows that any struggle against the abuse of language is a sentimental archaism, like preferring candles to electric light or hansom cabs to aeroplanes. Underneath this lies the half-conscious belief that language is a natural growth and not an instrument which we shape for our own purposes’.

The algorithm first encrypts the sensitive text data (Text) with the secret public RSA key “11,3”. Note in this software implemented that the button “Embed Data” will not be active if the video frame capacity is not able to carry all the encrypted bits. The result of concealing the secret data in this proposed 2-layer system is embedded

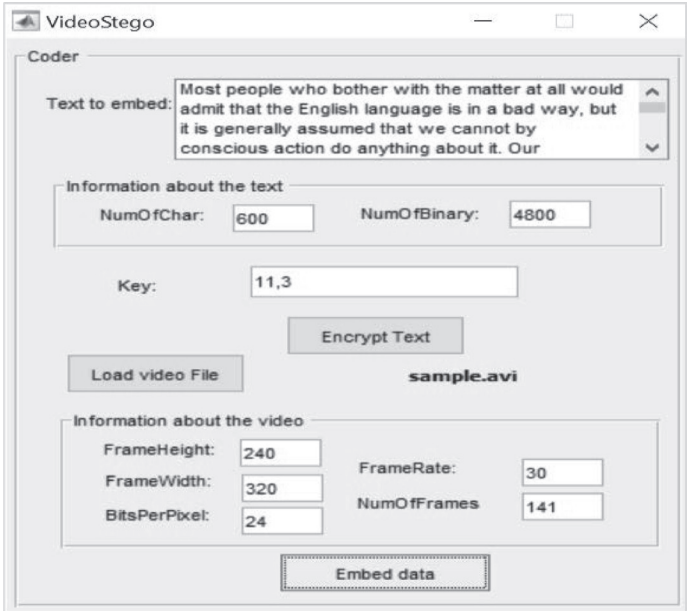


Fig. 3. Proposed system interface illustrating bits statistics and process framework starting by RSA encryption layer followed by the video based steganography

into the cover stego video frame.

The interface shown in Figure 4 can be used as an example of retrieving sensitive data that was hidden using the proposed 2-layer security system. By pressing the button "Decrypt Text" the program will operate retrieving back the secret sensitive text data. It starts by sensing the LSBs within the stego video frame collecting the bits together forming the ciphertext. Generating the ciphertext is representing reversing the stego layer process. Then, the ciphertext needs the secret key as inputs to the reverse RSA crypto layer that decrypts the ciphertext generating back the secret sensitive data message, following Fig. 4 the process of retrieving back secret text data.

V. Results Analysis & Comparison

The secret sensitive text message "Text" is encrypted and then hided within 15 different videos, as introduced before, in order to be analyzed and compared. To clarify this elaboration, we selected 15 differently sized PC cover-videos and noted the results. Table I lists the results of this experiment for 15 differently selected PC videos. The security testing study hided sensitive, concealed in videos cover resulting in bits changed based on the LSB choice used as listed in the Table I. These results made up the percentage computation of security and capacity per video using the security of each video as calculated using PSNR (Peak Signal to Noise Ratio) based on the formula:

$$PSNR = 20\log_{10}\frac{MAX}{\sqrt[2]{MSE}} \quad (1)$$

Where MAX refers to the maximum intensity of the given resolution of each pixel, i.e. this MAX value in the images is 255. On the other hand, MSE is defined as the square of the difference (distortion) between the original cover and the stego cover. The difference within the cover can be measured using this MSE by the formula below:

$$MSE = \sum_{i=0}^{allpixels}\sum_{j=0}^{allpixels}\frac{(cov(i,j)-steg(i,j))^2}{m\times n} \quad (2)$$

The capacity per video, i.e. stego cover-media, is estimated as the amount of information that can be hidden in the video file without significantly changing it. It is measured according to the cover that is used. The following formula illustrates the metric:

$$capacity = \frac{(number\ of\ characters)\times 8}{number\ of\ bits\ in\ image}\times 100 \quad (3)$$

This work studied the effect of using the 2-layer system to hide the secret text in PCs assuming security and capacity. All tests considered hiding, i.e. stego-embedding the encrypted fixed sensitive data "Text" in 15 different videos using different LSBs. The selected LSBs

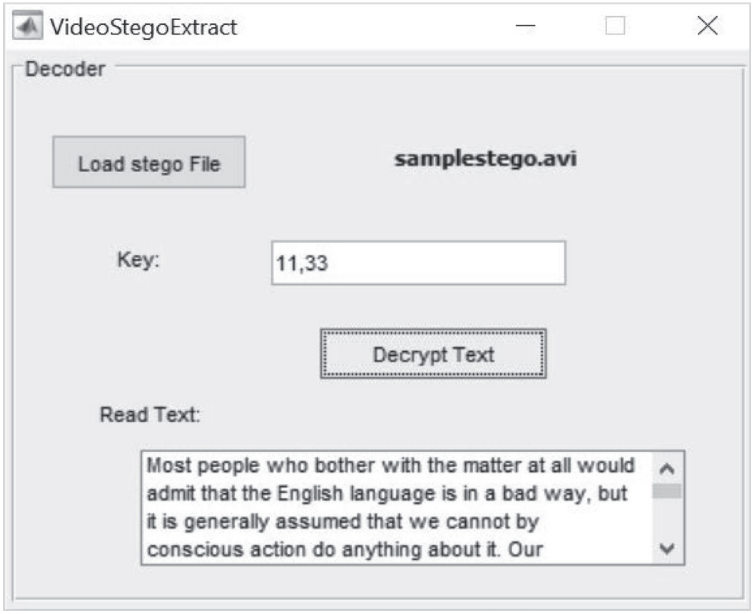


Fig. 4. The interface of retrieving the sensitive data using the proposed system.

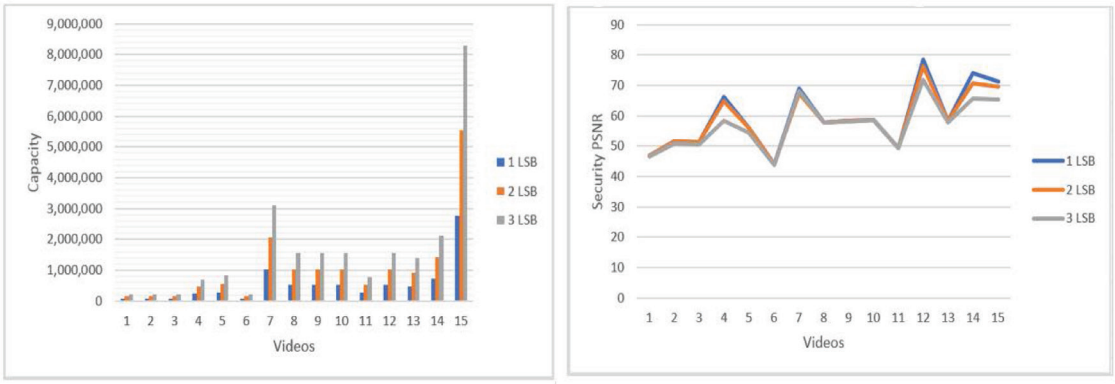
are 1LSB, 2-LSB, 3-LSB to conceal the secret text into in different videos providing different results for every video, as listed in Table I. The LSB used is directly proportional to the security and inversely proportional to the capacity. As the number of bits to hide data increase (1LSB, 2-LSB, 3-LSB) the capacity increase and security reduces, as clearly noted by 1-LSB: High security and low capacity, 2-LSB: Medium security and medium capacity, 3-LSB: Low security and high capacity, as shown in the Table I.

The results of the security and capacity of videos after hiding the secret text in different LSBs is presented in Fig. 5. It is to be noted from it, that the real indication of security and capacity is completely reliant on the LSB used and videos obtainable within the PC and cannot be predicted nor foretell it. Every cover-video is showing the percentage of security result based on the specific LSB used. As shown in Fig. 5 when increasing the number of LSBs to conceal the secret text the security will be decreased. On the other hands, the capacity of the amount the data can be hidden in video cover file will be increase when increasing the LSBs. In addition, the size of the cover video has a different effect on security and capacity when concealing one text. Observe in Fig. 5 that video "12" with 1-LSB is giving the highest security percentage to hide the secret text. This is despite the fact that there is another cover with better capacity, namely "15" with a frame size of 1280×720. Notice from the results that the cover "12" of size 480×360 is the best with respect to PSNR, and that cover "6" of size 176×144 is the worst with respect to security and capacity.

Using 2-LSB steganography as the stego layer capability increased the capacity of hiding information with acceptable security less than that for 1-LSB. It is to be noted from Fig. 5, that video "6" is giving the lowest security percentage to hide the secret data. The video "12" is the best choice to conceal the text according to the values of PSNR. Notice that the video "12" is also the best choice for the user when he is using 3-LSBs. Our work used 3-LSB in the stego layer to increase the capacity of the hidden sensitive text than when used 2-LSBwith considering the security still be acceptable and no one can notice there is a hidden data in the video cover.

The differences of values for the security and capacity between videos cover give the user the opportunity to take advantages of this flexibility to select the appropriate cover for concealing the secret text.

On the other hand, a comparison between this work and others using the same functionality of 2-layers cyber security for PC data hiding is given via different methods. The work compared covering data of our video steganography with image steganography taken from [1] and the results are listed in Table II. Note that Table 2 is measuring 5 images as well as 5 videos hiding the same encrypted text, i.e. same text in 5 different PC files, adopting two media types. After concealing the text and



a) Capacity b) PSNR

Fig. 5. a) Capacity and b) PSNR values, respectively, when hiding one text using different videos of different sizes.

TABLE I
TESTING RESULTS OF STEGO-EMBEDDING THE ENCRYPTED FIXED SENSITIVE DATA "TEXT" IN 15 DIFFERENT VIDEOS

Videos	Video Size	Frame Size	1-LSB High security and low capacity		1-LSB High security and low capacity		1-LSB High security and low capacity	
			Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
1	419 KB	176×144	76,032	46.86	152,064	46.85	228,096	46.61
2	447 KB	176×144	76,032	51.67	152,064	51.62	228,096	50.82
3	544 kB	176×144	76,032	51.39	152,064	51.33	228,096	50.46
4	464 KB	320×240	230,400	66.14	460,800	64.65	691,200	58.33
5	716KB	352×288	280,800	56.20	561,600	56.10	842,400	54.46
6	212 KB	176×144	76,032	44.11	152,064	44.09	228,096	43.82
7	887 KB	720×480	1,036,800	69.12	2,073,600	67.21	3,110,400	68.11
8	5.01 MB	480×360	518,400	57.78	1,036,800	57.73	1,555,200	57.66
9	2.25 MB	480×360	518,400	58.37	1,036,800	58.30	1,555,200	58.19
10	4.05 MB	480×360	518,400	58.75	1,036,800	58.63	1,555,200	58.48
11	2.09 MB	360×240	259,200	49.45	518,400	49.42	777,600	49.38
12	2.62 MB	480×360	518,400	78.49	1,036,800	76.23	1,555,200	71.91
13	3.27 MB	480×320	460,800	58.39	921,600	58.30	1,382,400	57.72
14	5.00 MB	640×368	706,560	73.99	1,413,120	70.73	2,119,680	65.69
15	5.00 MB	1280×720	2,764,800	71.20	5,529,600	69.62	8,294,400	65.39

TABLE II
COMPARING RESULTS OF STEGO-EMBEDDING IMAGES VS VIDEOS FOR SAME ENCRYPTED FIXED SENSITIVE DATA "TEXT"

Image Steganography				Video Steganography			
Images	**Size**	**Capacity**	**PSNR**	**Videos**	**Frame size**	**Capacity**	**PSNR**
each-eye	100×100	44,761	45.73	**1**	176×144	228,096	46.61
Sunset	60×90	24,168	40.39	**2**	176×144	228,096	50.82
Graduate	120×90	48,177	46.30	**3**	176×144	228,096	50.46
fly-bird	50×50	11,183	35.68	**4**	320×240	691,200	58.33
Coffee	70×100	31,760	50.56	**5**	352×288	842,400	54.46

running the tests, the results shows interesting promising values of capacity and security making video based as a valid choice over images for PC data cyber security. It is found that using this video security technique as a cover file is giving the user more capacity to hide text unpredicted more than the image cover. In addition, the security will be more better when using video as cover than using image, see the results listed in Table II.

This comparison indicates that our proposed method gives the user the full ability to secure the sensitive text within the PC assuming that RSA algorithm is working well (practical) when the text is short [19]. If the text is long, the passwords key transformation problem raise pointing out key management trouble needing consideration [20] as well as distribution of the keys and its secret sharing protocols as can be also a burden needing assistance [21]. These issues made up the advise to look for other efficient applicable encryption algorithms rather than RSA. In other words, whenever the user needs to hide large text files, RSA algorithms may degrade the PC performance [22], i.e. according to the complexity of the RSA algorithmic nature. Consequently, light weight cryptography [23] is the recommended cryptography option to handle these passwords and computational complexity burden [24]. Adoption of light weight cryptography needs further study considered as open future work following this research.

VI. CONCLUSION

This research presented a crypto-stego 2-layer security system for hiding encrypted text data within video files on personal computers. An RSA cryptography layer is used to insure PC independent security and then the steganography layer is adopted to give control to the user as fully dependent based on the PC data available. The system is simulated using MATLAB platform where the detailed statistical interface is given showing both steps as proposed in the process. The study has been focusing on a fixed sensitive data to be hidden via steganography in different video files, assuming high, medium, and low, options of security as well as capacity. All testing results have been considered stressing on the data dependency based on the video file options providing interesting results.

The system cryptography layer is fixed for the sensitive data. However, the steganography layer embedded encrypted data in different videos using several LSB attempts for every video. This variation of video steganography gave interesting enhancement in capacity vs. security tradeoff, allowing the user and application to be the decision maker in the choice. In fact, the study showed the possibility of accepting security of 1-LSB, 2-LSB, and 3-LSB methods and their effects. The system MATLAB elaboration focused on a study the effects on security when secured the data in different cover videos files used on the PC by examining the same secret data to be hidden on 15 differently size videos showing interesting attractive results.

As future work, this combined RSA cryptography video based steganography 2-layer system is to be improved by varying the crypto layer. Different crypto methods, symmetric as well as asymmetric, are to be tested and compared. Also, planning is to be done to study different other ways to enhance the capacity and the security of the system for personal use with PC applications. The system can be further improved to support other languages and their features, which may need some more focused research.

Acknowledgment

The authors would like to thank Umm Al-Qura University (UQU) for aiding this research. Thanks also to Shaqra University for this wonderful cooperation giving Miss Nouf Al-Juaid the chance to be teaching assistant and grant her to continue her MS in the field of information security at UQU – Makkah.

References

[1] N. Al-Otaibi, and A. Gutub, "2-Leyer Security System for Hiding Sensitive Text Data on Personal Computers," *Lect. Notes on Inf. Theor.,* vol. 2, no. 2, pp. 151-157, June 2014, doi: 10.12720/lnit.2.2.151-157.

[2] N. Al-Otaibi, and A. Gutub, "Flexible Stego-System for Hiding Text in Images of Personal Computers Based on User Security Priority," in *2014 Int. Conf. Adv. Eng. Technol. (AET-2014)*, Dubai, UAE, pp. 250-256.

[3] A. Gutub, "Pixel Indicator Technique for RGB Image Steganography," *J. Emerg. Technol. in Web Intell. (JETWI)*, vol. 2, no. 1, pp. 56-64, Feb. 2010, doi: 10.4304/jetwi.2.1.56-64.

[4] N. Al-Otaibi, A. Gutub, and E. Khan, "Stego-System for Hiding Text in Images of Personal Computers," presented at *The 12th Learning and Technol. Conf.: Wearable Tech/Wearable Learn.*, JD, KSA, Apr. 2015.

[5] A. Gutub, & H. Tahhan, "Improving Cryptographic Architectures by Adopting Efficient Adders in their Modular Multiplication Hardware," presented at *The 9th Annu. Gulf Inet. Symp.,* Khobar, KSA, Oct. 13-15, 2003.

[6] S. Gupta, A. Goyal and B. Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography," *Int. J. Mod. Educ. and Comput. Sci. (IJMECS),* vol. 4, no. 6, pp. 27-34, 2012, doi: 10.5815/ijmecs.2012.06.04.

[7] Deepli, "Steganography With Data Integrity," *Int. J. Comput. Eng. Res.,* vol. 2, no. 7, pp. 190-193, Nov. 2012.

[8] P. R. Deshmukh and B. Rahangdale, "Hash Based Least Significant Bit Technique for Video Steganography," *Int. J. Eng. Res. and Appl.,* vol. 4, no. 1, pp. 44-49, Jan. 2014.

[9] K. Singh, "Video Steganography: Text Hiding in Video by LSB Substitution," *Int. J. Eng. Res. and Appl.,* vol. 4, no. 5, pp. 105-108, May. 2014.

[10] H. Gupta and S. Chaturvedi, "Video Steganography through LSB Based Hybrid Approach," *Int. J. Eng. Res. and Develop.,* vol. 6, no. 12, pp. 32-42, May 2013.

[11] N. Prabhakaran and D. Shanthi, "A New Cryptic Steganographic Approach using Video Steganography," *Int. J. Comput. Appl.,* vol. 49, no. 7, pp. 19-23, Jul. 2012, doi: 10.5120/7639-0722.

[12] H. A. Aly, "Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error," in *IEEE Trans. Inf. Forensics Secur.,* vol. 6, no. 1, pp. 14-18, Mar. 2011, doi: 10.1109/TIFS.2010.2090520.

[13] P. Praveen, and R. Arun, "Audio-video Crypto Steganography using LSB substitution and advanced chaotic algorithm," *Int. J. Eng. Inventions,* vol. 4, no. 2, pp. 01-07, Aug. 2014.

[14] A. Swathi and S.A.K Jilani, "Video Steganography by LSB Substitution Using Different Polynomial Equations," *Int. J. Comput. Eng. Res.,* vol. 2, no. 5, pp. 1620-1623, Sept. 2012.

[15] S. K. Moon and R. D. Raut, "Analysis of secured video steganography using computer forensics technique for enhance data security," in *2013 IEEE Sec. Int. Conf. Image Inf. Process. (ICIIP-2013),* Shimla, pp. 660-665, doi: 10.1109/ICIIP.2013.6707677.

[16] P. Badhak and B. Gunjal, "Improved Protection In Video Steganography Using DCT & LSB," *Int. J. Eng. Innov. Technol. (IJEIT),* vol. 1, no. 4, pp. 31-37, Apr. 2012.

[17] A. Gutub, "Merging GF(p) Elliptic Curve Point Adding and Doubling on Pipelined VLSI Cryptographic ASIC Architecture," *Int. J. Comput. Sci. Netw. Secur.,* vol. 6, no. 3, pp. 44-42, Mar. 2006.

[18] N. Goshwe, "Data Encryption and Decryption Using RSA Algorithm in a Network Environment," *Int. J. Comput. Sci. and Netw. Secur.,* vol. 13, no. 7, pp. 9-13, Jul. 2013.

[19] A. Gutub and E. Khan, "Using Subthreshold SRAM to Design Low-Power Crypto Hardware," *Int. J. New Comput. Architect. and Appl.,* vol. 1, no. 2, pp. 474-483, 2011.

[20] L. Ghouti, M. K. Ibrahim and A. Gutub, "Elliptic Polynomial Cryptography with Secret Key Embedding," U.S. Patent 8351601, Jan. 8, 2013.

[21] A. Gutub, N. Al-Juaid and E. Khan, "Counting-Based Secret Sharing Technique for Multimedia Applications," *Multimed. Tools Appl.,* vol. 78, no. 5, Nov. 2017, doi: 10.1007/s11042-017-5293-6.

[22] M. Rahman, T. Saha and A. Bhuiyan, "Implementation of RSA Algorithm for Speech Data Encryption and Decryption," *Int. J. Comput. Sci. Netw. Secur.,* vol. 12, no. 3, pp. 74-82, Mar. 2012.

[23] N. AlAssaf, B. AlKazemi and A. Gutub, "Applicable Light-Weight Cryptography to Secure Medical Data in IoT Systems," *J. Res. Eng. Appl. Sci. (JREAS),* vol. 2, no. 2, pp. 50-58, Apr. 2017.

[24] L. Ghouti, M. K. Ibrahim, and A. Gutub, "Method of Generating a Password Protocol Using Elliptic Polynomial Cryptography," U.S. Patent 8332651, Dec. 8, 2012.