American Journal of Applied Sciences

Review

A Proposed an Enhanced Authentication and Dual Encryption Algorithm: Secured Video Transmission in Surgical Tele-Training

[1]Anil Wagle, [1]Abeer Alsadoon, [1]P.W.C. Prasad, [1]Linh Pham and [2]A. Elchouemi

[1]School of Computing and Mathematics, Charles Sturt University, Sydney, Australia
[2]Colorado State University Global Campus, USA

Article history
Received: 12-10-2018
Revised: 07-12-2018
Accepted: 26-12-2018

Corresponding Author:
P.W.C. Prasad
School of Computing and Mathematics, Charles Sturt University, Sydney, Australia
Email: Cwithana@studygroup.com

Abstract: Implementation of tele-training for trainee surgeons has been slow to date as current standards of video transmission do not meet requirements for security, speed and clarity for such videos. The aim of this paper is to increase security by providing enhanced authentication as well as improving the overall throughput of the system. The proposed solution consists of a dual encryption algorithm based on Elliptical curve cryptography and 2k-RSA which enhances security through entropy and also performance through the processing time. It reduces the key size of the algorithm to reduce encryption and decryption time. Furthermore, two-factor authentication using biometrics and a secure One-Time Password (OTP) are used for authentication. Results show that the proposed algorithm reduces processing time by 33% for encryption and 43% for decryption compared to the current best solution, while entropy increased by 11% during encryption.

Keywords: Encryption, RSA Algorithm, Elliptical Curve Cryptography Security, Authentication, Surgical Training System

Introduction

Training material in the medical field is often based on authentic records of treatments, particularly in the area of surgery where video recordings permit the detailed study of surgical processes through 'pause' and 'replay' functions, augmenting and to some extent replacing physical presence in the operating theatre. Although participation in surgery delivers effective training according to Suzuki *et al*. (2005), there is little room for practice except when assisting an expert surgeon where opportunities for hands-on surgery are restricted. Furthermore, there are limitations in terms of the number of trainee-surgeons experts can train at a time. Furthermore, such processes require trainees to be physically present making the training time-consuming and costly.

Recent experimentation with augmented reality in the operating theatre has led to advancements in the development of sophisticated video recordings that permit virtual cooperation between a local surgeon and an expert (Suthakorn, 2012). The resulting recordings, if augmented with teaching comments, become appropriate self-study training material allowing trainee surgeons to become theoretically proficient in carrying out procedures prior to a significantly reduced period of hands-on training (McLaughlin, 2001; Suthakorn, 2012).

Such Tele-training systems provide secure virtual training rooms where experts and trainee surgeon can come together even though they are physically in different locations (Suthakorn, 2012). However, there are challenges to implementation, particularly in the medical field, as videos taken during surgery record highly sensitive material requiring high security. In addition, there is a need for superior speed during transmission and clarity in terms of performance. To overcome these issues, secure pre-transmission authentication and high entropy are needed to provide the appropriate security. Furthermore, video quality must be high, requiring that the system does not degrade the clarity of transmission.

Current surgery training systems apply new network technologies (i.e., 5 g); new authentication schemes based on multimodal authentication and combinations of different encryption techniques for secure data transmission. The challenge is to achieve high security without compromising throughput (Webster, 2017).

The purpose of this research is to increase the security of video transmissions by reducing the key size

of the RSA algorithm while reducing computational cost. Current RSA algorithms require the addition of extra keys for a higher level of security which is here overcome through an enhanced RSA algorithm for video encryption based on 2k-RSA with Security card (Seca) as additional security (Alslaity and Tran, 2017). Furthermore, the introduction of biometrics with a secure One-Time Password (OTP) as mentioned by Yadav (2017) enhances the existing authentication scheme.

Related Work

Authentication in Surgical Tele-Training Systems

File sharing online is vulnerable to attack particularly during the authentication process.

Tiwari *et al*. (2016) combined a password biometric and a smart card to overcome threats from 'the man in the middle'. This combination offers acceptable levels of security but depends on password storage, thus creating a further vulnerability. This was overcome by Roy (2016) who investigated a secure OTP to eliminate human error from the authentication process. This is based on Pretty Good Privacy (PGP) and SHA512 generated by the system. This work is useful to the proposed solution as this form of password generation is fast and does not require password storage. However, as it can be breached with attacks from 'brute force', enhancements are required before it functions as intended.

Similar research was carried out by Yadav (2017) for banking transactions. This included a combination of Elyptic Curve Cryptography ECC and biometrics to facilitate encryption of the OTP significantly enhancing the security of OTP. However, the solution must be used with dual authentication because the OTP can be breached by 'brute force attack'; therefore, we implement OTP with fingerprint biometrics.

Data Encryption for Tele-Training Systems

The speed with which data are encrypted and decrypted has significant impact on the efficiency of such systems.

Harba (2017) measured the impact of time on the encryption of data in file transfers and authorization systems combining three algorithms (RSA, AES, HMAC) to achieve an encryption time of under 0.5 seconds. Whilst this is an improvement over other current solutions of around 1 second, the cost is high which is undesirable. Hussain (2016) approached the video quality issue through the Peak Signal to Noise Ratio (PSNR) using noise aggregation which leads to 126.7 dB PSNR in the main channel. If the wiretap channel is improved, then the video suffers from a passive attack. The passive attack in the surgical system can lead to false result and degradation of performance, which is considered fatal.

Hayajneh (2015) achieved 1.1 Mbps processing time for Wireless LAN (WLAN) of WPA2 in IOT systems based on an enhanced WPA2 scheme. This is an improvement over 1.9 Mbps achieved so far but devices must be online for encryption making the system inappropriate for the proposed work.

The impact of encryption on visual resemblance of images in the video stream was the subject of the work of Kumari (2016). The researchers used dual encryption based on RSA and ECC algorithm which produced near 0% visual resemblance. Whilst this is an improvement over current solutions of 'slight' resemblance, the RSA algorithm requires additional keys for higher security. We enhance the RSA using 2k-RSA in our proposed solution.

Network Performance in Surgical Tele-training Systems

Liu (2015) investigated throughput and security for transmission of multimedia data in IOT systems using Virtual Private Network (VPN) with L2TP tunnel using AES encryption leading to 4.67 Mbps throughput. Whilst this is an improvement over current solutions with 5.80 Mbps throughput, the AES algorithm creates performance degradation. Therefore, it is unsuitable for the proposed system. Further research by Tozal (2013) into the reliability of video and audio transmission in wireless telesurgery provides both secure and adaptive reliability using SSR-UDP. The scheme provides 99% reliability even with high packet loss. Although this is an improvement over current solutions with less than 90% reliability, the system must recover the corrupted packets which create performance degradation due to discontinuous transmission which is not acceptable for the proposed system.

Kiah (2014) measured the impact of traffic on the usage of a CPU in real-time video conferencing using group communication architecture which led to 15% CPU usage in encrypted traffic compared to 18% in other current solutions. However, the key generation process significantly increases encryption time and thus overheads. This is, therefore, of no further interest.

Wickramage (2016) investigated information misuse and its impact on the privacy of records in health care systems using an auditing framework that leads to secure data protection. However, the researchers did not account for human error. This paper is, thus, of no further interest.

Jevdjic (2017) examined errors in encrypted videos in storage. Using approximation, they achieved a bit rate error of 10-3. However, the modification in the Cipher block chain encryption can propagate to the next block which may the error which, thus, propagates from the encryption to the decryption phase which is undesirable.

El Kalam (2016) conducted research into the impact of security and latency of networks in a bilateral teleoperation system on Q-IPSec leading to 110 ms latency. The system provides QOS and throughput twice as high as traditional IPsec with 150 ms latency.

However, IPSec is not supported by IPv6 and, thus, not suitable for the proposed solution as everything is switching towards IPv6.

Duong (2017) measured the impact of congestion on the throughput of data in Internet-based robot system time. They used Real-Time Protocol (RTP) with Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) which achieved 700kbps throughput. Whilst this is an improvement over current solutions with 500 kbps, the TCP does not provide congestion control which creates high jitter, undesirable for critical applications.

Ramakrishna (2017) explored the impact of Quality Of Service (QOS) on the traffic of video streams in future internets which reduced network traffic to 50%. This led to improvements, but a problem exists with the Dijkstra algorithm which is simple and breakable and could compromise the whole system.

Current Best Solutions

The current best solution is a hybrid solution and the work of Tiwari *et al*. (2016) and Nalawade *et al*. (2017). Tiwari *et al*. (2016) introduced an authentication method that uses a secure OTP to limit unauthorized access. This has been combined with a method for transmitting real-time videos using dual encryption to provide security against tampering (Nalawade *et al*., 2017). The current best solution consists of a source and a destination site. Figure 1 illustrates techniques and methods used for the system. Desirable features are highlighted in blue and limitations are shown in red.

Source Site (Trainer Surgeon)

Video transmission is generally initiated by entering a username to establish a connection between the remote users. At the source site, the trainer must log on to the system with a username – a unique identity. The system then creates a secure OTP which is encrypted using an asymmetric key. The public key is used to encrypt the OTP to generate a cipher text. The destination site (trainee surgeon) follows the same registration process. To view the teaching material, the trainee surgeon also requires an OTP which will be sent to their mobile.

This system has limitations in the authentication phase as the process is based on a single factor (username) which generates an OTP vulnerable to 'brute force' attack.

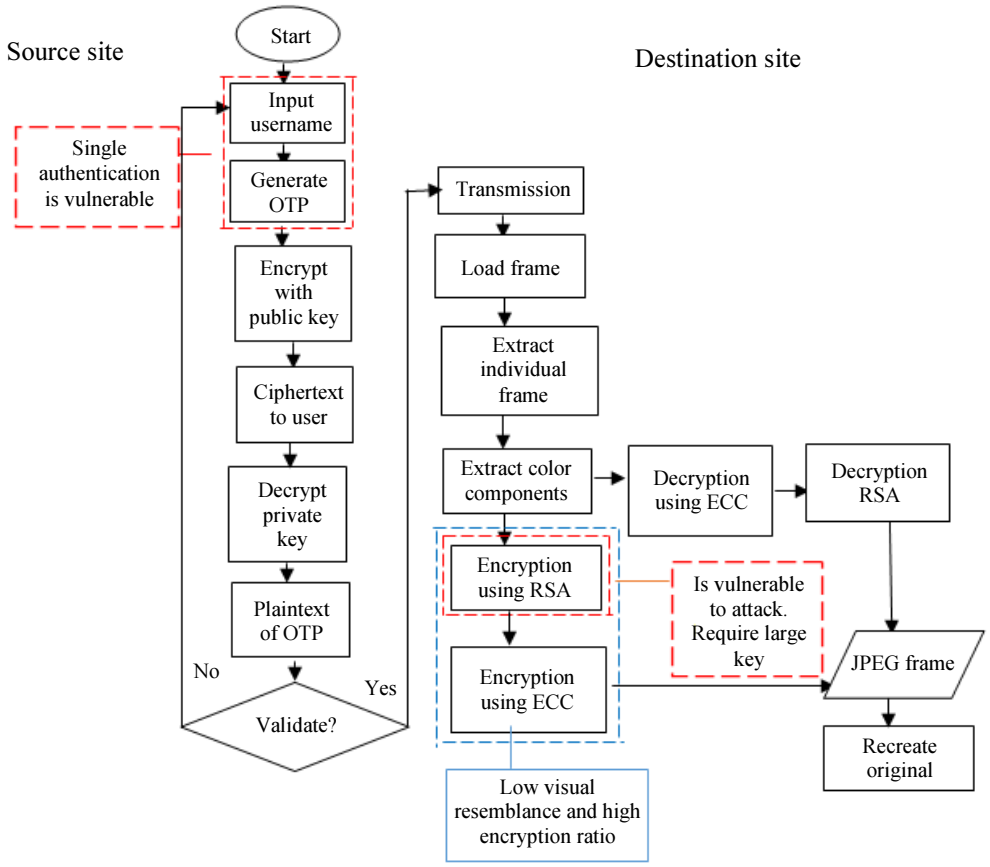

Fig. 1: This figure depicts: (a) the flowchart of the current video encryption of surgical tele-training system (Nalawade *et al*., 2017) and (b) the merits (blue) and demerits (in red) of the current video encryption in a surgical tele-training system

Destination Site (Trainee Surgeon)

The training video material is first encrypted using an RSA algorithm followed by a further encryption using ECC. The original frame is loaded onto the system. Each individual frame is extracted one by one and converted into color components consisting of red (R), green (G) and blue (B). These R, G, B components are encrypted using ESS in Level 1 and RSA algorithm in Level 2. Finally, the encrypted color components are combined into a JPEG frame to generate an encrypted video.

The medical student accesses the training video from a remote location by logging onto the system which is once more divided into individual frames. The R, G, B components are extracted from each frame and decrypted using ECC followed by RSA decryption. The decrypted color components are combined into JPEG frames which are combined to obtain the original video as shown in Fig. 1.

This model proved secure with good performance as the dual encryption provided low visual resemblance compared to other solutions. An encryption ratio of 16% was achieved using dual encryption compared to the single scheme using RSA. The encryption and decryption speed remained under 0.19. This solution provides authentication to limit access to an unauthorized user. The low visual resemblance leads to lower similarity between the encrypted and original frame and, therefore, higher security in terms of the overall video transmission. However, the major issue is the use of the traditional Rivest-Shahmir-Adelman (RSA) algorithm which requires a large bit of key for achieving a high level of security.

This demand for a high key size leads to a decrease in the overall performance as encryption and decryption time increases. In case of training involving critical surgery, time delays may lead to image distortions (Nalawade *et al*., 2017). Further limitations were found in the authentication phase based on a single factor namely the username which generates an OTP which is generally considered secure. However, the password can be deciphered using ‘brute force’ (Roy, 2016). The dual encryption algorithm based on RSA and ECC are depicted in the flowchart is shown in Fig. 2.

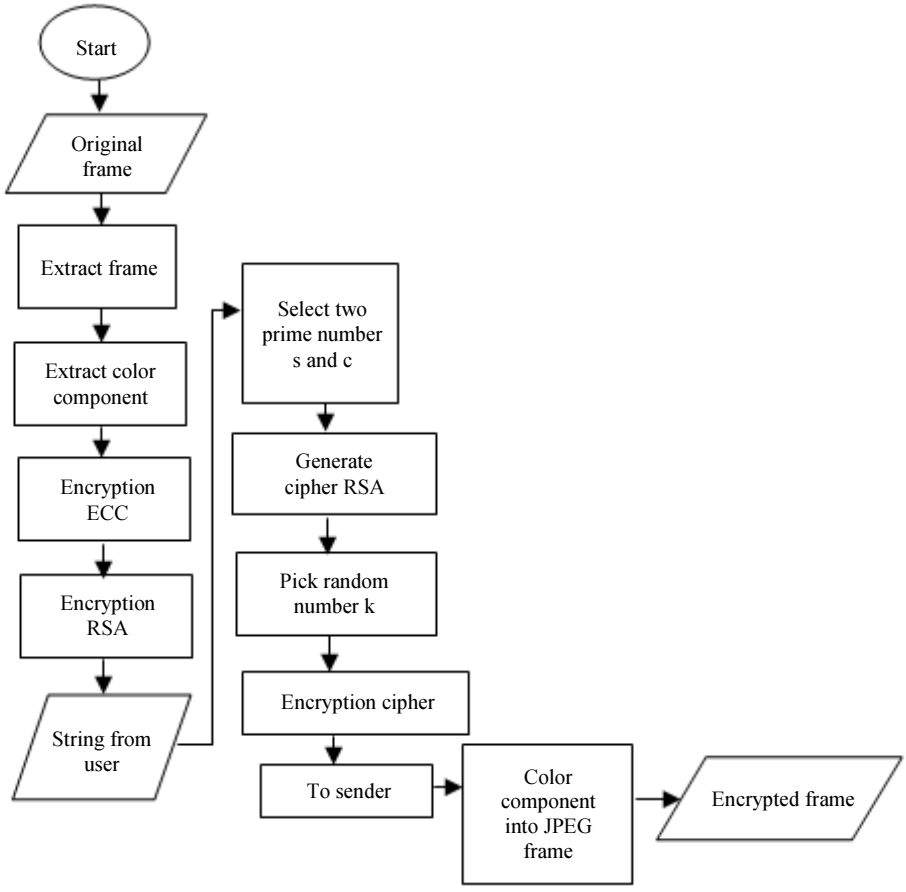

Fig. 2: Flowchart for Dual Video Encryption ECC and RSA showing the working process of the current video encryption security of video in the surgical tele-training system

The ciphertext which is generated using a dual encryption algorithm can be calculated with Equation 1 (Kumari, 2016):

$$E_{rsa} = (C_T)k + 1 \quad (1)$$

Where:
E_{rsa} = The encrypted ciphertext
C_T = The output of RSA encryption
k = The parameter both known to sender and receiver
RSA = Encrypted ciphertext (C_T) is given by Equation 2 (Kumari, 2016):

$$C_T = \left(M_{sg}{}^{E} mod\ n\right) \quad (2)$$

Where:
M_{sg} = the message sent from the sender
E = The encryption key
n = A big prime number

Proposed Solution

This review of current research has identified authentication and secure data transmission over a real time network as the main issues. The proposed solution is based upon the best current solution (Kumari, 2016) with an enhanced RSA algorithm and a security card to overcome the issues relating to security and performance. A further enhancement was the addition of a biometrics feature in the authentication step and a dual key RSA algorithm with Security Card (2k-RSA) is used to reduce the key size, thus improving encryption speed and overall throughput of the surgical tele-training system (Alslaity and Tran, 2017).

We propose a new method for enhancing the RSA algorithm by using a 2k-RSA algorithm with Seca. The 2K-RSA algorithm uses two keys for encryption and decryption, see Fig. 3. The sender generates two public and two private keys. The message is also divided into m1, m2. This algorithm is faster because it uses two smaller keys compared to one large 1024 bit key for the RSA.

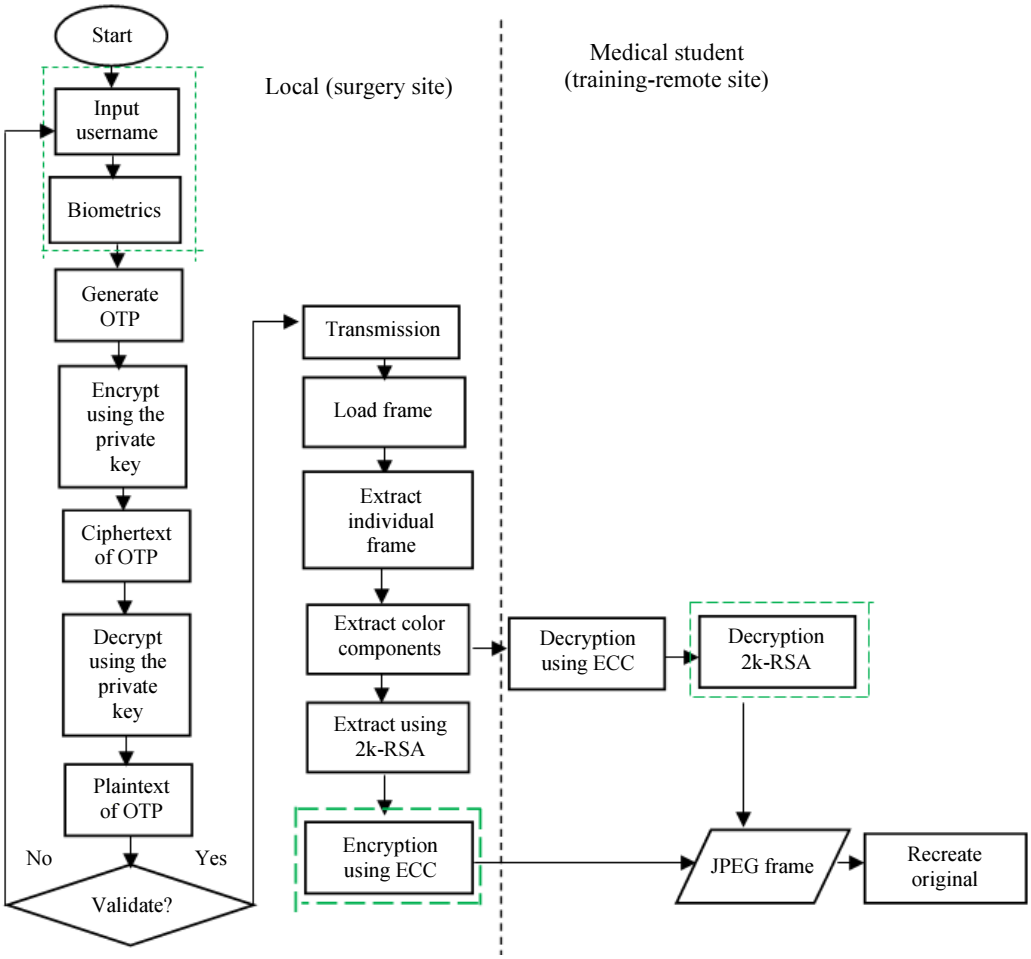

Fig. 3: The Proposed surgical tele-training system based on 2k-RSA (Alslaity and Tran, 2017) and Biometrics (Yadav, 2017) for enhanced security in the surgical tele-training (local surgery site has biometrics and 2k-RSA encryption added to the solution) and the enhanced features are highlighted in green

The security component Security Card (SeCa) has information on the position of the encrypted cipher text as well as the encryption keys. The use of SeCa provides additional complexity to block attackers intending to decrypt the cipher text. To completely access the cipher text, the attacker must also have the position of the cipher text in addition to the correct order of the composite cipher making an attack unlikely. The proposed solution encrypts the training video using 2k-RSA with SeCa and ECC before transmission to the trainee surgeon in the remote location (Alslaity and Tran, 2017). Furthermore, the authentication introduced by Yadav (2017) before the actual transmission is enhanced using the biometrics fingerprint of the user.

The RSA algorithm was introduced by Rivest-Shamir-Adleman (RSA) in 1978 based on an asymmetric algorithm. Two keys are generated during the process – a public key which is announced publicly and a private key that is with the sender. The entire algorithm is built from two large prime numbers. Typically, the sender has the private key and announces the other key publicly. The other entity can encrypt the message using the public key. The receiver then uses the private key to decrypt the message. The primary phases of the RSA algorithm include: Key Generation, Encryption and Decryption. For a higher level of security in the RSA algorithm, a single 1024-bit key is considered the most secure option. However, issues arise when selecting a larger number to generate a single large key. This key is considered highly secure, but the increase in key size will increase the encryption and the decryption time by a factor of eight (Alslaity and Tran, 2017). Therefore, the performance of the entire system is compromised. To overcome this issue, the RSA algorithm was refined by several researchers through a range of process steps.

The final outcome - an enhanced solution - requires a username together with its biometrics fingerprint as introduced by Yadav (2017), to identify the sender, here the expert surgeon (the trainer) who logs on to the system using his username and biometric fingerprint.

Source Site

Initially, the surgical training system requires a username to establish a connection between the remote users. To initiate the process, the trainer surgeon registers with a username in the system. This username is his unique identity. The system then creates a secure OTP which is encrypted using the asymmetric key. The public key is used to encrypt the OTP to generate a cipher text according to Roy (2016). Once the trainer has identified himself to the system, he provides the trainee surgeon at the destination site with a video taken during a real surgical procedure augmented for training purposes. The video is first encrypted using a 2k-RSA algorithm and then encrypted using ECC as in Equation (1). The original frame is loaded onto the system. All frames are extracted one by one and converted into colour components consisting of Red, Green and Blue. This R, G, B components are encrypted using ECC in Level 1 and 2k-RSA algorithm in Level 2. Finally, the encrypted colour components are combined in a JPEG frame to generate an encrypted video. The 2k-RSA with SeCa (two-key-based RSA algorithm with security card) generates a composite cipher as the result of the multiple encryption keys.

Destination Site

The trainee surgeon also registered using their username and biometric fingerprint to generate a secure OTP at the destination site. To view the live surgery and teaching material, the trainee surgeon requires the OTP which will be sent to his mobile by the system. After successful authentication by the system, the receiver requests the video. The previously encrypted video is loaded on the system. The system divides the video into individual frame and the R, G; B components are extracted from each individual frame and applied to the ECC. Then the ECC decrypted colour components are applied to 2k-RSA with SeCa decryption. Now the original message is obtained using the private key. The composite message Msg is Msg [m1, m2, SIK]. Where m1 and m2 are part to the message and SIK is the segment information key used to decrypt the Segment Information Cipher (SIC). The decrypted color components are stored in a frame to generate an original video which is finally displayed to the trainee surgeon for educational purposes.

Areas of Improvement

Proposed modifications centre on the initial prime number selection for the RSA algorithm. The current RSA algorithm uses a large key for more security. However, the increase in key size increases encryption time and creates a system overhead. We propose an algorithm similar to the RSA, the only difference being that the key is divided into two 512 bits (k1, k2) and uses a security card to calculate the position of the cipher text for secure generation. The message M is also divided into two parts m1 and m2 so that k1 is used to encrypt m1 to generate c2 and k2 is used to encrypt m2 to generate c2. The length of ciphertext c1, c2 is calculated together with M and encrypted using SIK (segment identification key) to generate the position of the ciphertext. The ciphertext [c1, c2, SIC] is concatenated to generate the whole cipher.

The first major contribution of this proposed solution is enhancing the key generation using dual encryption for maximum security. Strong encryption and efficient key generation algorithms will fend off brute force attacks which the simple RSA in the current solution cannot facilitate. The use of 2k-RSA with Security Card has the advantage that there are now two small keys of

512-bit RSA rather than a single 1024-bit RSA key. Two keys (k1 and k2) are generated and the message is divided into two parts (m1, m2) and stored in a two-dimensional array. The SIC parameter determines the actual position of the cipher text obtained by concatenating c1 and c2 and the SIC parameter.

Proposed Equation

The 2k-RSA enhanced with ECC generated following ciphertext as specified by proposed Equation 3:

$$E_{2k-rsa} = \left([c1, c2, SIC]\right)\ k+1 \tag{3}$$

Where:

$E_{2k\text{-}rsa}$ = The encrypted ciphertext using enhanced dual encryption
k = The parameter both known to sender and receiver,
([$c1$, $c2$, SIC]) = The enhanced ciphertext generated by 2k-RSA algorithm
$c1$ = The first part of composite cipher (C_T) equation
$c2$ = The first part of composite cipher (C_T) equation 2
SIC = The segment information cipher which contains information about the ciphertext

The enhanced ciphertext generated in Equation (3) by 2k-RSA, which originated from the state of art solution (Kumari, 2016). The ciphertext (C_T) in Equation 2 was modified using 2k-RSA with SeCa algorithm. The final ciphertext generated in Equation 2 was divided into two parts ($c1$, $c2$) and an extra component SeCa was added to it. Which generated the enhanced ciphertext $\left([c1, c2, SIC]\right)$ see equation 4:

$$c1 = m1^{e1}\ mod\ n \tag{4}$$

Where:

$c1$ = The first part of composite cipher (C_T) Equation 2
$m1$ = The first part of message M_{sg} Equation 2
$e1$ = The first part of the key E Equation 2
n = A big prime number

Ciphertext1 is calculated by Equation 5 (Kumari, 2016):

$$c2 = m2^{e2}\ mod\ n \tag{5}$$

Where:

$c2$ = The first part of composite cipher C_T as derived in Equation 2
$m1$ = The first part of message $M_{sg,}$ Equation 2
$e1$ = The first part of the key E equation 2
n = A big prime Number

The proposed Equation (3) solves the issue with security in Equation 1 (Kumari, 2016) as a security card (Seca) is induced in the scheme. The main use of Seca is that it contains a detail of the encryption process, keys and message segment. Seca adds complexity to the decryption process as the attacker must retrieve the original format and in the correct order. Additional time is required to find the information for the ciphertext stored in Segment Information (SI) which forces the attacker to retrieve the information byte by byte requiring excessive amounts of time and a significant number of trials.

Dividing the Message (Msg) into two parts and key(E) in Equation 2 (Kumari, 2016) into two parts has the benefit that the key size is reduced. Using a RSA 1024 bit is same as using 2×512-bit (2k-RSA) scheme in terms of processing time and security (Alslaity and Tran, 2017).

The main limitation of the current best solution is the large key size in the current RSA algorithm. The RSA algorithm uses a 1024 bit key for maximum security. The use of a large key RSA l results in low performance of the overall system as the encryption of the key requires a significant amount of time. The proposed equation will solve this issue by using two keys and dividing the message into two parts to generate two ciphers in a 2D matrix. The added security component SeCa has the location of the cipher text (Alslaity and Tran, 2017).

Why 2K-RSA?

The RSA generation uses a single large prime number constituting the single large key. The underlying principle is that the higher the size of the key, the more secure the encryption. Therefore, a key using 1024 bits is considered highly secure. However, an increase in key size lengthens the process of the key generation by a factor of 16 and that of encryption by a factor of 8 and so on. Furthermore, RSA alone is vulnerable to brute force attack. This justifies modification of the existing RSA-scheme using two 512-bit keys and addition of a secure component - a Security Card. The use of two keys has the advantage that the size as the key remains small, but the level of security is high. Therefore, 1024-bit RSA key-based security is equal to two 512-bit 2k-RSA based security. The 2k-RSA has two public keys and two private keys. Furthermore, the message is divided into two parts and stored in a 2-D array.

Encryption key1 is used together with message1 to generate cipher text and similarly, key 2 is used together with message 2 to generate cipher text 2. The Security Card has information about encryption and key generation. The Security component has information on the position of cipher text in the 2-D array (SIC). The use of the added security component makes the decryption process harder. Even if attackers have the cipher text, decryption is still not possible because position and order of the cipher text is still not known. Therefore, the 2k-RSA is a secure encryption algorithm which improves the security of video transmission (Alslaity and Tran, 2017).

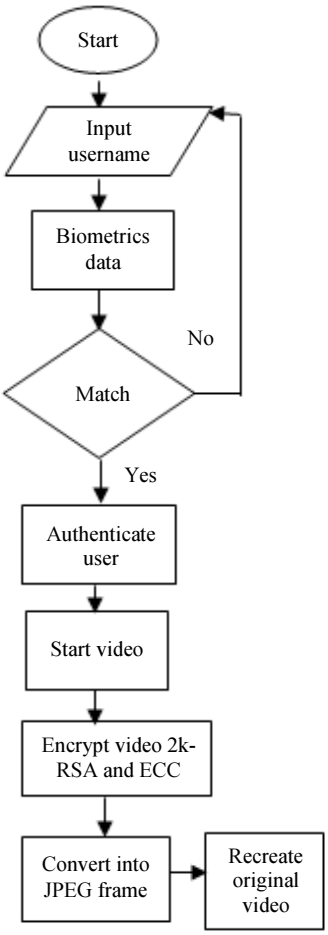

Fig. 4: Flowchart of the enhanced video encryption algorithm 2k-RSA with SeCa

Table 1: Pseudo code of video encryption enhanced through using a 2k-RSA with SeCa in the proposed solution

Algorithm 2K-RSA with SeCa **INPUT:** Message **OUTPUT**: CIPHERTEXT
BEGIN Step 1: Load Message (M_{sg}) into 2-D array Step 2: Divide Message(M_{sg}) into two parts (m1, m2) Step 3: Use Key1(e1) and Key2(e2) and ENCRYPT {m1, m2} to get Cipher text {c1, c2} Step 4: Generate Segment Information Cipher (SIC) Step 5: Generate full cipher using Equation 4 Step 6: Encrypt using Elliptical Curve Cryptography as Equation 1 END

The Fig. 4 depicts the flowchart of the proposed solution and Table 1 gives the pseud code of it. At first a username is input followed by biometric information. If the latter is a match, then the video is encrypted and transmitted. At the decryption site, the original video is converted to frames.

Experimental Results

GNS2 network simulator[24] and Linux 14.04[25] was used during the simulation and implementation of the proposed model. GNS2 simulator was used for was used for implementation and simulation of the proposed solution using 10 real-time knee replacement surgery sample and open-heart surgery sample videos of two patients of different age group. The video sample taken for test varied in length from 6 to 8 min and the number of frames was 30 fps. Both real-time surgery sample video was taken from free online sources for the educational purpose. These samples are available in YouTube channels for the educational purpose. The original sample video was extracted as individual frame. Each individual frame varies in image size and resolution and all video frames extracted with MATLAB were considered for a result as in Table 2 and 3. The extracted frame samples were encrypted and decrypted using proposed equation 3. The result of were evaluated and compared based on frame size, resolution, entropy and processing time for both encrypted and decrypted frame depicted in Table 2 and 3. The entropy and processing time as the state of art solution and proposed solution were compared. The result from the simulation is depicted in Table 2 and 3.

We have compared the result from the knee surgery video sample the entropy and processing time to the frame transmitted via real time network were compared the entropy calculated from the state of art and proposed solution were compared. Similarly, the processing times required for the encryption and decryption of the frame were compared. Both parameters were compared based on frame size and resolution. In the local surgery site, the processing time for each individual frame is compared together with the entropy it produced. Similarly, at the remote site when individual encrypted frames are decrypted the processing time is compared together with the entropy.

Samples of individual video frames from knee and open heart surgery were compared using the current best and the proposed solution (Fig. 5). Results are shown in Tables 2 and 3. Results are categorized according to encryption/decryption phase, with entropy and processing time being the main parameters.

Entropy (image randomness) is a key requirement due to the sensitive nature of the material. Entropy must be achieved through the encryption process to obscure structure and is measured based on randomness. It defines the measure of the unpredictability of bits in information on the system. In terms of security, entropy must be applied to the cipher text to hide the amount of structure that is visible in the original image. The higher the entropy the more secure the encryption. The ideal entropy must be in the range of 8.

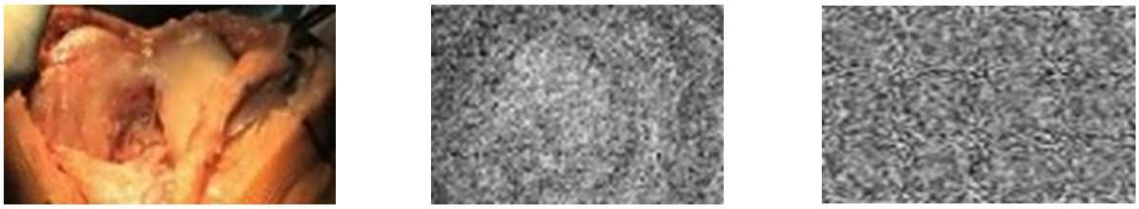

Fig. 5: Depicts an image sample (here knee surgery). The left image shows the original frame; the central image represents encryption using the current best solution; the image on the right is the encrypted frame using the proposed solution

Table 2: Entropy and Processing time of State of Art and Proposed solution (The entropy increased by 0.25% compared to the state of art solution in Knee Replacement Surgery sample with a duration of 6 min and 30 frames per second)

	Video sample			State of Art						Proposed					
	Original Frame			Encryption			Decryption			Encryption			Decryption		
No.	Frame	Frame size(KB)	Resolution	Frame	Entropy	Processing Time(ms)	Frame	Entropy	Processing time	Frame	Entropy	Processing Time(ms)	Frame	Entropy	Processing Time(ms)
1		7.69	480*270		7.393	5.8631		6.2921	4.6921		7.9921	3.8515		6.2921	3.0999
2		11.4	540*336		7.89	6.9001		5.6054	5.1920		8.0056	4.13699		5.6054	3.9748
3		13.3	640*320		7.2322	6.9999		6.1212	4.9245		7.8956	4.3148		6.1212	2.5141
4		21.7	540*320		6.9898	8.2231		5.3452	5.9889		8.2367	5.4341		5.3452	3.8928
5		12.38	640*320		7.5738	7.6128		6.5466	6.7005		7.9560	5.928		6.5466	4.355
6		98.8	680*900		6.4678	25.5671		5.6671	14.8945		8.1234	19.2913		5.6671	9.4314
7		81.2	720*540		7.9948	20.6749		5.2348	10.7898		8.2005	17.6059		5.2348	8.4634
8		63.4	740*360		7.001	17.8569		6.0001	9.6772		7.9900	15.2189		6.0001	7.6901
9		37.2	720*390		6.9729	12.2845		5.9791	7.2924		8.0563	8.2991		5.9794	5.8451
10		10.4	800*260		6.2345	5.2134		5.5790	4.5678		7.8090	3.1029		5.5790	2.9691
Average		11.72	540*360		7.175	11.72		7.472	7.472		8.025	8.719		7.472	5.224

Table 3: Entropy and Processing time of State of Art and Proposed solution (The entropy increased by 0.25% compared to the state of art solution in open heart surgery sample with duration of 8 min and 30 frames per second)

	Video sample			State of art						Proposed					
	Original Frame			Encryption			Decryption			Encryption			Decryption		
No.	Frame	Frame Size(KB)	Resolution	Frame	Entropy	Processing Time(ms)	Frame	Entropy	Processing time	Frame	Entropy	Processing Time(ms)	Frame	Entropy	Processing time (ms)
1		8.67	480*270		5.9987	6.2633		5.0045	5.6921		8.1194	4.3217		5.0045	3.69 67
2		11.4	640*360		6.8061	8.2676		5.9925	6.8927		8.0414	5.7047		5.9925	4.4775
3		18.36	640*320		7.12	8.9271		6.546	7.0245		8.3771	6.1597		6.5461	4.5659
4		16.7	640*320		6.882	12.0966		6.0456	7.5889		8.1456	8.3467		6.0456	4.8929
5		19.38	640*320		7.2345	14.0321		6.239	8.0005		8.5431	9.6822		6.2390	5.2003
6		8.3	480*270		5.4178	6.0671		4.3451	5.1945		7.9929	4.1863		4.3451	3.3757
7		20.0	720*540		7.2948	14.3749		6.983	8.2898		8.0013	9.6059		6.983	5.2528
8		22.4	640*360		7	15.3569		6.544	8.6772		8.29	10.2189		6.5441	5.6402
9		27.2	570*390		7.7729	17.8845		7.0001	8.9924		8	12.299		7.0001	5.8451
10		10.4	420*360		6.4345	8.1134		5.7889	5.9678		8.1121	5.9029		5.7889	3.8691
Average		16.28	640*320		6.796	11.14		6.049	7.232		8.163	7.643		6.049	4.791

Processing time is important because if the processing time is high, the training material may no longer be identical to real-time surgery. Processing time is calculated as the time required for encryption of an individual frame based on key generation (public and private).

Other parameters considered are frame size and resolution of each individual frame. Overall, ten samples were tested.

Average results for both measures were calculated and depicted in Fig. 6, 7, 8 and 9 to show the increase in entropy and decrease in processing time for the proposed solution.

The result was compared during the encryption and decryption stage of the video transmission for samples from knee replacement and open-heart surgery. The proposed solution shows improved results for entropy and a decrease in processing time.

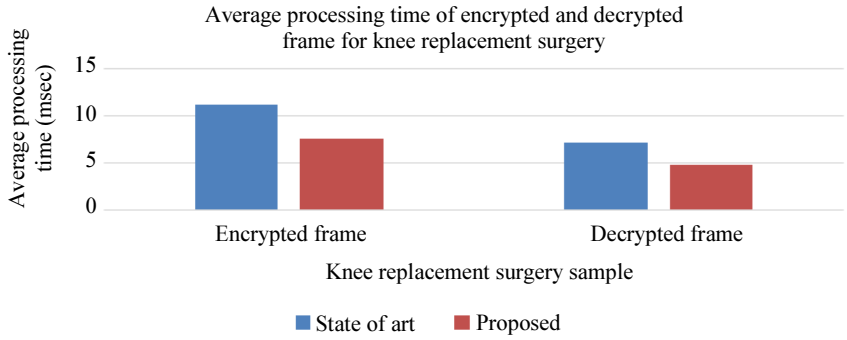

Fig. 6: This figure shows the average processing time for frame encryption as 11.72 (existing solution) and 8.791 (proposed solution) and 7.472/5.224 respectively for frame decryption (knee replacement samples)

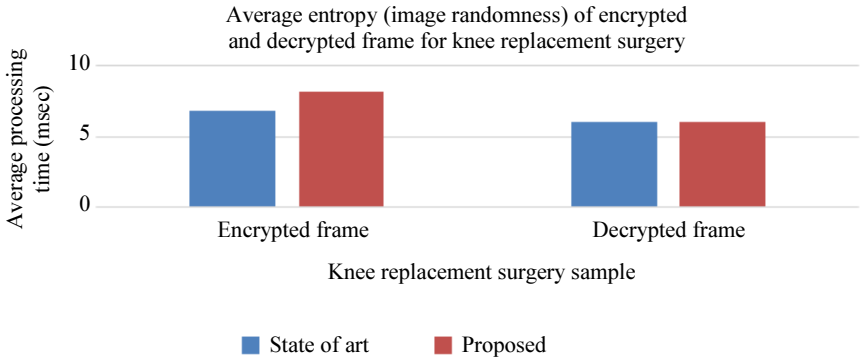

Fig. 7: The average entropy of an encrypted frame is 7.175 (existing solution) and 8.025 (proposed solution) average entropy of both state of art and proposed is 7.427 as in both the original frame is recreated

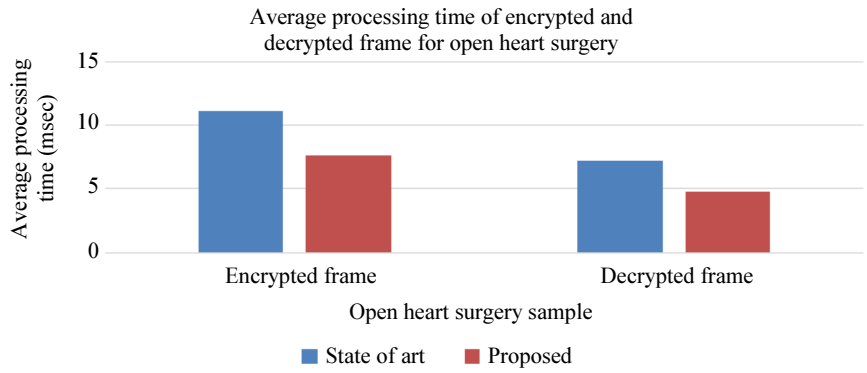

Fig. 8: For video frames showing open heart surgery, different levels of complexity led to slightly different results: 11.14 (existing solution) and 7.643 (proposed solution) and the average processing time for frame decryption was 7.232 and 4.791 respectively

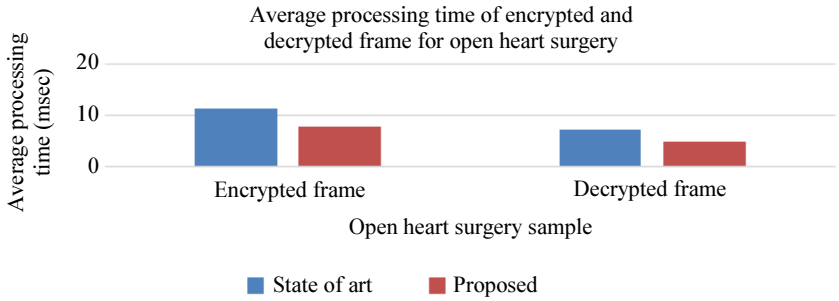

Fig. 9: The average entropy of an encrypted frame is 6.796 (existing solution) and 8.163 (proposed solution) average entropy of both state of art and proposed is 6.049 as in both the original frame is recreated

Discussion

Results show the difference in entropy and processing time between the existing and the proposed solution during encryption and decryption video frames taken live during surgery. Outcomes demonstrate that the proposed solution based on Alslaity and Tran (2017), has improved the entropy by 26% over the best existing solution. A high degree of randomness has been achieved with no similarity remaining between the original and encrypted frames. This work has overcome the limitation of the state of the art solution in terms of processing time, reducing average times for frame encryption from 11.72 in the state of the art solution to 8.791 in the proposed solution and also 7.472 and 5.224 respectively. It means, 31% less in encryption time and 35% less in decryption time as depicted in Table 2 and 3 and Fig. 6. Processing time was calculated by simulating Equation 1 (existing solution) and the proposed Equation 6.

Similarly, average entropy of an encrypted frame improved from 7.715 in the current best solution to 8.025 in the proposed solution and the average entropy of both the state of the art and the proposed solution is 7.427 as in both solutions the original frame is created, as shown in Fig. 7. Entropy was calculated using the entropy function available in MATLAB. We quantified the degree of improvement in processing time by both algorithms simultaneously for each individual frame and recorded the time required to encrypt and decrypt the original frame.

Alslaity and Tran (2017) have proposed a solution with 2k-RSA which has two public and two private keys. The message is divided into two parts and stored in a 2-D array. For encryption, key1 is used together with message1 to generate the cipher text and, similarly, key 2 is used together with message 2 to generate cipher text 2. The Security Card has information about encryption and Key generation. The Security component has information on the position of the cipher text in the 2-D array (SIC). The use of the extra security component makes the decryption process harder. For example, even if the attacker has the cipher text, they still cannot decrypt it because they must also have the cipher text in the correct order and must know the position of the cipher text. Therefore, it is a secure encryption algorithm which improves the security of video transmission.

The proposed system has been tested in a MATLAB simulator. The result has shown a reduction in processing time during the video transmission which increases the performance of the video. The proposed solution also considers the security of the video in transit making it unavailable to unauthorized access with the help of a strong encryption technique.

Conclusion

To sum up, the combination of different existing solutions led to the creation of a greatly improved surgical tele-training system. The dual encryption offers high security for sensitive material in transit so that unauthorized users are denied access to the material. The introduction of an OTP verifies the authentic users of the system.

Although a range of techniques is available for video encryption, they have not been implemented as higher security requires more encryption and, therefore, more processing time. These are two major factors that need to be addressed when implementing the surgical tele-training system. This research has facilitated opportunities for overcoming the limitations of the current best solution which had high processing time in decryption and encryption of the real-time surgery video. The introduction of 2k-RSA with SeCa has reduced the processing time to 35 and 31% respectively, which has justified the addition of the proposed 2k-RSA algorithm to overcome the limitations and increase performance of the overall surgical training system.

The proposed solution implemented in MATLAB has proven to decrease the processing time of the encryption and decryption process to 31% and 35% respectively. The addition of biometrics input has improved the authentication of the system. The overall entropy of the video sample increased after the encryption. The increase in entropy ensured that the

original as well, the encrypted video revealed no similarities and, therefore, made it harder to decrypt for an outside attacker. Table 3 provides comparative results between the state of art and proposed solution.

Future research needs to be conducted into further improvements of the encryption and decryption time by introducing a more efficient algorithm which will improve the overall speed of the system. Furthermore, biometrics may benefit from the inclusion a multimodal authentication scheme including iris and retina scans.

Acknowledgement

We are grateful to Mrs. Angelika Maag for proof reading and making corrections to this article. Without her support, it would have not been possible to submit this in the current form.

Author's Contributions

Anil Wagle: She has completed this project as part of his MIT degree program.

Abeer Alsadoon: Worked on the setup of the experiments and gave important suggestions on design of experiments. In addition to, as Abeer Alsadoon is the main supervisor on this work, she provided the details guidelines and feedback in each step of this work.

P.W.C. Prasad and Linh Pham: Made important revisions to most sections of the paper.

A. Elchouemi: Done the technical review of the paper and provided technical guidance. Give the final review and approval for the manuscript to be submitted.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and there are no ethical issues involved.

References

Alslaity, A. and T. Tran, 2017. An enhanced cryptosystem based on shorter keys and new security component. Int. J. Comput. Applic., 166: 44-50. DOI: 10.5120/ijca2017914150

Duong, P.M., 2017. Control of an internet-based robot system using the real-time transport protocol. arXiv preprint arXiv, 1707.05456.

El Kalam, A.A., 2016. Bilateral teleoperation system using QOS and secure communication networks for telemedicine applications. IEEE Syst. J., 10: 709-720. DOI: 10.1109/JSYST.2015.2422992

Harba, E., 2017. Secure data encryption through a combination of AES, RSA and HMAC. Eng. Technol. Applied Sci. Res., 7: 1781-1785.

Hayajneh, T.U., 2015. An enhanced WLAN security system with FPGA implementation for multimedia applications. IEEE Syst. J., 11: 2536-2545. DOI: 10.1109/JSYST.2015.2424702

Hussain, M., 2016. Security enhancement for video transmission via noise aggregation in immersive systems. Multimedia Tools Applic., 75: 5345-5357. DOI: 10.1007/s11042-015-2936-3

Jevdjic, D., 2017. Approximate storage of compressed and encrypted videos. Proceedings of the 22th International Conference on Architectural Support for Programming Languages and Operating Systems, Apr. 08-12, ACM, Xi'an, China, pp: 361-373. DOI: 10.1145/3037697.3037718

Kiah, M.M., 2014. Design and develop a video conferencing framework for real-time telemedicine applications using secure group-based communication architecture. J. Med. Syst., 38: 133-133. DOI: 10.1007/s10916-014-0133-y

Kumari, P., 2016. Dual-layer video encryption using RSA and ECC algorithm. Int. J. Scientific Res. Publicat., 6: 620-625.

Liu, C., 2015. Study on a secure wireless data communication in internet of things applications. Int. J. Comput. Sci. Netw. Security, 15: 18-23.

McLaughlin, M.I., 2001. Telesurgery and surgical simulation: Haptic interfaces to.

Nalawade, C.V., S.N. Sayyad and P.S. Sutar, 2017. Dual-layer video encryption and decryption using RSA algorithm. Int. J. Adv. Res. Ideas Innovat. Technol., 3: 817-820.

Ramakrishna, M., 2017. SIP and SDP based content adaptation during real-time video streaming in future internets. Multimedia Tools Applic., 76: 21171-21191. DOI: 10.1007/s11042-016-4017-7

Roy, S., 2016. Towards designing and implementing a secure One Time Password (OTP) authentication system. Proceedings of the IEEE 35th International Performance Computing and Communications Conference, Dec. 9-11, IEEE Xplore Press, Las Vegas, NV, USA, pp: 1-2. DOI: 10.1109/PCCC.2016.7820604

Suthakorn, J., 2012. A concept on cooperative Tele-surgical system based on image-guiding and robotic technology. Proceedings of the Pan American Health Care Exchanges, Mar. 26-31, IEEE Xplore Press, Miami, FL, USA, pp: 41-45. DOI: 10.1109/PAHCE.2012.6233437

Suzuki, S., N. Suzuki, A. Hattori, M. Hayashibe and K. Konishi, 2005. Tele-surgery simulation with a patient organ model for robotic surgery training. Int. J. Med. Robot., 1: 80-88. DOI: 10.1002/rcs.60

Tiwari, M., S.S. Panda and G.P. Biswas, 2016. An improved secure remote login protocol with three-factor authentication. Proceedings of the 3rd International Conference on Recent Advances in Information Technology, Mar. 3-5, IEEE Xplore Press, Dhanbad, India, pp: 372-378. DOI: 10.1109/RAIT.2016.7507932

Tozal, M.E., 2013. Adaptive information coding for secure and reliable wireless telesurgery communications. Mobile Netw. Applic., 18: 697-711. DOI: 10.1007/s11036-011-0333-3

Webster, N., 2017. Surgeons to get better feel for remote operations when 5G technology rolls out.

Wickramage, C., 2016. Anatomy of log files: Implications for information accountability measures. Proceedings of the 18th International Conference on e-Health Networking, Applications and Services, Sept. 14-16, IEEE Xplore Press, Munich, Germany, pp: 1-6. DOI: 10.1109/HealthCom.2016.7749426

Yadav, D., 2017. Intensify the security of one time password using elliptic curve cryptography with fingerprint for e-commerce application. Int. J. Eng. Sci.