Journal of Science and Technology, Vol. 42, No. 2 (2024), pp 50 - 63

https://dx.doi.org/10.4314/just.v42i2.4

STEGOVIDEO: AN EFFICIENT MECHANISM FOR SECURING VIDEO DATA USING STEGANOGRAPHY AND CRYPTOGRAPHY TECHNIQUES

Oluwafolake E. Ojo[1], Morenikeji K. Kareem[1], Ibrahim K. Ogundoyin[2], Olufunke A. Oyinloye[3] and Oluwapelumi L. Ikumpayi[1]

[1]Department of Computer Science, Federal University of Agriculture, Abeokuta, Nigeria
[2]Department of Computer Science, Osun State University, Osogbo, Osun State, Nigeria
[3]Department of Computing, University of Ilesa, Ilesa, Osun State, Nigeria.

Corresponding author: ojoeo@funaab.edu.ng

ABSTRACT

The COVID-19 pandemic episodes have rapidly expanded multimedia systems utilization across the globe. Nowadays, practically all companies and educational systems rely predominantly on streaming platforms. Owing to the popularity of online streaming; it is crucial to secure video. Although, a few techniques have been deployed to guarantee secured video transmission. Nonetheless, the recent usage of video applications due to the pandemic poses more security risks such as losing sensitive video content to intruders. In this paper, a hybrid framework (named StegoVideo) is proposed for securing video information by consolidating the best components of RSA encryption and LSB steganography procedures. This strategy guarantees that videos with sensitive information are imperceptible by intruders because the encoded video is introduced in the form of images and is converted back to videos when decrypted. Our experimental results revealed that StegoVideo is a proficient method for securing video content on the Internet.

Keywords: Video Streaming, RSA, Steganography, Security, Internet.

INTRODUCTION

The news of the recent pandemic cases came as a surprise to the world when announced officially by the World Health Organization as a novel coronavirus which led to total lockdown in major countries across the world and disrupted daily activities (Moshin *et al*., 2021). This COVID-19 occurrence plays a major role in Internet-based multimedia systems as a mechanism for supporting virtual working, e-learning, online social interaction, e-transaction, streaming audio or video, and many more (Favale *et al.,* 2020). With the quick advancement of different multimedia systems, more real-time videos are produced and communicated in the clinical, business, and military fields which might incorporate some sensitive data that ought not to be accessed by unapproved users. Therefore, security and privacy are required for video streaming (Gutub and Al-Ghamdi 2020). From research, it has been discovered that hackers or attackers are now adopting sophisticated tools for attacking information systems as technology is advancing. Vital or confidential information can now be easily compromised or altered to suit evil desires especially when transferring from one network to another (Yaacoub *et al*., 2020). Videos can also be hijacked by attackers if not properly secured. Video is now one of the major targets of attackers, people can easily be manipulated by what they see than written text, (Sam *et al.,* 2023). Fake or manipulated information or video could bring down a nation or cause defamation. Consequently, there arises a need to apply efficient security measures to videos while sharing or transferring from one network to another. This paper adopts a hybrid method to provide proper security for videos transferred from networks. Many researchers have adopted the method of steganography to secure data but this method is not efficient for video data, (Roselinkiruba, R., & Hemalatha 2023), this paper combines steganography and cryptography methods to efficiently secure video data. A video is audiovisual content; it is envisioned as a sequence of image frames showing at a high rate alongside motion data which can likewise contain the sound component (Kumar & Chaudhary 2016). The digital visual information is typically coordinated in rectangular arrays indicated as frames, the components of these arrays are signified as pixels or picture components (Alhassan *et al.,* 2018).

Generally, streaming is the process of conveying media content either audio or video from a server over a network or Internet to an individual or group of clients. In this situation, the audio or video contents are not saved on the customer's devices. However, the multimedia contents are viewed by the customer's application programs because it is conveyed at a predefined rate (Duan *et al*., 2020). The video streaming components comprise essentially the streaming server and the customer's software. The major role of the streaming server is to stream the audio and video data in a standard real-time format and is furthermore liable for dealing with the customer's solicitations to access hosted media data. Similarly, the role of the customer's application programs is perusing the received real-time packets and decoding them to the particular codes for legitimate viewers (Almadani *et al*., 2016). According to the literature, video-on-demand (VoD) and live videos are the main types of video streaming. Live video streaming represents real-time occurrences such as live events and sports, live meetings, and live teaching which are streamed continuously. VoD on the other hand is On-request data delivery, the videos are pre-recorded and stored on the video server. Every customer initiates their streaming session; hence, nobody at any point comes in late to the streaming session (Abd-Elrahman & Boutabia 2010).

Cryptography is the traditional approach to protecting transmitted data or stored

information. It is a bunch of cycles or capacities utilizing keys to encode plain text such that; the content is meaningful to the targeted recipients alone (Alabdullah *et al.,* 2021). In cryptography, the process of transforming the original data (such as text, picture, sound, and video) into indiscernible, imperceptible, or garbled format during transmission is called encryption (Rabah, 2005), in a nutshell; encryption is a method of converting data or information into a mysterious code. Encryption is one of the effective techniques for accomplishing video data security; a private or secret key is usually required to decrypt video data (Kumar & Chaudhary 2016). Information encryption and decryption is as yet probably the best procedure for getting data secrecy and decency. Ultimately, there is a foremost test as weaknesses and perils are developing with the upgrade of advances (Mondal & Goswami 2021). Steganography has been observed to be a significant and generally utilized act of concealing a message, picture, audio, or video data into another non-secret information. In the conventional approach, individuals utilized undetectable ink to compose something mysterious on customary paper that is steganography. Recently, the pattern of digit files has changed the course of steganography (Liu & Chen 2020). Steganography technique has been developing quickly based on its viability in keeping others from endeavouring to decrypt the secret data hidden in the cover data (Gutte *et al*., 2013); the main objective is to implant secret data into a cover medium with the reason for distinguishing proof, copyright insurance, and annotation. The primary limitation components of this process are message information quantity, and the need for constancy of embedded data under distortions like third-party removal, or modification (Duan *et al.,* 2020). Research showed that consolidating steganography with cryptography ordinarily offers solid security (Liu & Chen 2020). Hence, this research proposes a robust framework that guarantees powerful and proficient security and protection of video data on the Internet utilizing the blend of steganography and information encryption.

Related Work

Over the previous years, a few scientists have created many schemes for video security frameworks utilizing cryptography or stenography strategies. For instance, the process of encrypting real-time video applications into the scalable extension of the high-efficiency video coding (HEVC) standard, alluded to as SHVC was proposed by (Hamidauche *et al.,* 2017). The experimental investigation uncovered that encoding simply the least or entire layers achieved a great security level, in any case, encrypting the most noteworthy layer alone could diminish the quality of the most noteworthy layer (Hamidauche *et al.,* 2017). A commutative encryption and information concealing system for HEVC recordings was also introduced (Xu 2019). The commutative property permits encoding a stenographic video without meddling with the embedded signal or performing steganography on an encrypted video while as yet permitting wonderful decryption. The security investigation results exhibited and demonstrated that the scheme can accomplish insight security and cryptographic security.

Moreover, ViCrypt, a stream-based artificial intelligence mechanism for real-time forecasting from encrypted video real-time traffic was designed (Seufert *et al*., 2019). The scientific outcomes showed that the framework accomplished greater precision and accuracy. Nonetheless, for recall, system accuracy was lower, due to the profoundly poor dataset. Some other researchers designed a new video encryption mechanism using quantum video permutation. Through broad exploratory examinations, it was discovered that the approach can effectively

secure video-on-demand systems (Song *et al.,* 2020). An approach to enhance the embedding proficiency of LSB-based steganography was examined by (Abdulla *et al.,* 2019). The scheme introduced two distinctive secret bit-stream reversible methodologies that came about in an extension to a critical expansion in the proportion of 0s in the bit-stream. The secret image and cover pictures were tested using different scenarios to accomplish a large closeness between the bit-stream of the secret picture and the LSB plane of the cover picture.

The authors (Dalal & Juneja 2019) proposed a productive video steganography method for Standard Definition and High Definition video data. The method utilizes discrete wavelet transforms for concealing the secret information within the video chunks. The experiment conducted uncovered that the framework provides robustness against various sorts of noise attacks and distinctive compression levels which makes the system suitable for securing data. Furthermore, a two-level information concealing algorithm for video steganography was introduced by the authors (Manisha & Sharmila 2019). The algorithm gives two-level encryption, consequently to decipher the video data, how the secret image is initially decomposed and the frame in which it is embedded ought to be known.

In (Suresh & Sam 2020), a mechanism for hiding secret data in video sequences utilizing oppositional GreyWolf optimization was presented. The approach is capable of minimizing distortion and upgrading security to get prevalent video quality. The experiment conducted showed that the technique conveys greater security and limits distortions in video quality.

The researchers (Shanthakumari & Malliga 2020), consolidated Steganography and Cryptography strategies for shielding crucial data from attackers. The LSB Inversion Steganography algorithm and Elliptic Curve Cryptography (ECC) algorithm were deployed; the ECC algorithm was utilized to encrypt information while the LSB Inversion algorithm was utilized to embed encoded information into a cover picture. The results obtained through empirical investigation showed that the scheme accomplished better performance in securing data. In (Sengupta & Rathor 2020), a hybridized procedure was proposed, which incorporates Structural Obfuscate and Crypto-Steganography for securing JPEG equipment for clinical imaging frameworks against attacks like Trojan insertion and counterfeiting. The method assists with giving a twofold line of safeguard to secure JPEG CODEC and offers preventive control to the structural topology of the circuit by making it unclear for attackers to comprehend. The test results showed that this strategy acquired more prominent security comparable to the strength of obfuscation and strong stego-key size. In addition, the authors (Pramani *et al.,* 2020), combined cryptography and steganography strategies such that signature image information was concealed inside a cover image, this method requires the secret key of the sender and receiver to extract the data from the original information. This approach could be utilized to enforce data security; notwithstanding, it gave less distortion in the stego image.

The scientists (Kurniawan & Satrya 2021) likewise presented a mixture procedure through post-quantum cryptography and the LSB steganography strategy by changing the bit of the concealed picture with the message bit. The experimental result obtained showed that the approach could be adopted to secure banking cards, identity cards, and so on. In (Wahab *et al*., 2021), an approach of hybridization strategy was presented to improve the security level of data over the Internet from imposters. The scheme uses RSA cryptography and, lossy and lossless compressing steganography strategies. The scheme is equipped to diminish the time of transmitted data and storage space. The

Huffman coding algorithm was utilized for compacting the plain text, the cover image was compacted by discrete wavelet transform to diminish the cover picture measurements, and the LSB was utilized to embed the encrypted information. The performance result was high when contrasted with other frameworks. Moreover, a secure algorithm to transmit concealed images was designed (Akoum & Moughrabi 2020). The process includes a random selection of video by the sender, where the video data is divided into frame bytes with the end goal that bits of the secret video information will be shared among the frames. The concealed information sent is watermarked and modified using the LSB of the frame byte. The picture is converted into the binary matrix and moved using a distinct key to make the concealed message unobvious.

In (Solima *et al*., 2021), a secure high-efficiency video coding for HEVC steganography approach concealing an encrypted private audio message embedded in a compacted video frame in a protected way was presented. The discrete cosine transform was employed to compress the audio message to obtain an improved result for the steganography method. An encryption technique known as random projection and Legendre sequence in the discrete wavelet transform domain was used to encrypt the compressed secret audio message before implanting it within the HEVC frame. The methodology is safe and powerful in the presence of a steganalysis mixed media attack; however, it is significantly based on securing the audio message. The authors (Taurum *et al.,* 2020), introduced a strategy for concealing secret messages from intruders by embedding the message in a video to give a stego-video using the steganography method, the video transfer is supposed to be compacted to guarantee the safe transmission of the data over the communication medium. The stego-video is transferred to the recipient where the reverse of the implanting process is carried out to decode the stego item for the extraction of the secret message or original message. A method known as bits replacement was utilized to embed the secret message without loss of data. Lastly, steganography and cryptography methods were utilized to give protection and security to delicate data (Nyo & Oo 2019). The Arnold scrambling and discrete wavelet transform procedures were adopted for the secret picture, the encoded message is embedded inside the sound file utilizing the parity coding strategy.

Given the analysis of the related work in Table 1, data encryption or cryptography methods aren't adequate in securing video data transmission due to the detection of decrypting keys by attackers or unwanted users. Likewise, the blend of cryptography and steganography techniques has been demonstrated as probably the best methodology that can give a significant level of security in secret video data transmission across the Internet. Although some of the recent video security mechanisms in literature are capable of securing video data, nonetheless, the quality of the video after the decryption process may diminish. The point of this exploration is to apply the best components of cryptography and steganography procedures to guarantee an undeniable level of security for sensitive video data during transmission while retaining video quality.

Table 1: Analysis of the related work

Author	Technique	Pros	Cons(s)
Hamidouche *et al*., (2017)	Encryption solution for the scalable extension of the High Efficiency Video Coding (HEVC) standard.	minimal delay and complexity overheads	Encrypting only the lowest or all layers provides high security while encrypting only the highest layer leads to a perceptual encryption solution with slightly lower quality.
Abdulla *et al*., (2019)	Digital Steganography	minimal distortion, high embedding efficiency, and robustness	The approach only hides information in the image.
Dalal and Juneja (2019)	Video steganography adopting discrete wavelet transforms	high imperceptibility and robustness	Can only be adopted for securing secret messages only. Securing video was not considered.
Manisha and Sharmila (2019)	Steganography	a secret image is hidden in a frame of the video	Robustness was not considered
Shanthakumari and Malliga (2020)	LSB Inversion algorithm and the Elliptic Curve Cryptography algorithm	Only Securing hidden data into a cover object was considered	The approach does not consider securing videos.
Pramanik *et al*., (2020)	Combination of cryptography and steganography	They successfully hide signature image information into a cover image, It is easy to implement.	error detection and correction, Virtual quality and robustness were not mentioned
Wahab *et al*., (2021)	RSA cryptography with and compacting steganography	The method reduces the storage capacity and transfer speed	Complex to implement
Akoum and Moughrabi (2020)	Hamming code and LSB	The visual quality of the secret image is low after decryption.	The influence of the method on the size of the stego-image after encryption was not mentioned.
Soliman *et al*., (2021)	Discrete Cosine Transform (DCT) and Quaternion Fast Fourier Transform (QFFT)	Robustness is high	This approach only hides audio messages within video
Tarun *et al*., (2020)	LSB	The approach is simple to implement	Only text messages can be secured with the approach, The robustness and error rate were not stated.

METHODOLOGY

The StegoVideo architecture as displayed in Figure 1 comprises the key generation stage, hybrid process stage, and decoding stage. The StegoVideo framework is a hybridized approach that utilizes the RSA encryption and LSB steganography procedures to proficiently and adequately secure video streaming systems. At the sender's end, the original video is transmitted, which converts the original video to bytes and the RSA algorithm produces the public key for encrypting video data and the private key for decryption. The encrypted video is additionally hidden by utilizing the steganography technique, subsequently converting encrypted videos over to stego-images. The stego-images are received at the receiver end; these images are unhidden and decrypted back to the original video at the receiver end. For the first phase which is the key generation stage; the StegoVideo key generation process is represented in Algorithm 1. It adopts the principles of the standard RSA algorithm to create the encryption and decryption keys as shown in Lines 3-8 of Algorithm 1. The StegoVideo system also ensures that the variables representing the key features of the private keys are protected as represented in Line 10 of Algorithm 1; this is essential to ensure the confidentiality of the encrypted video data.

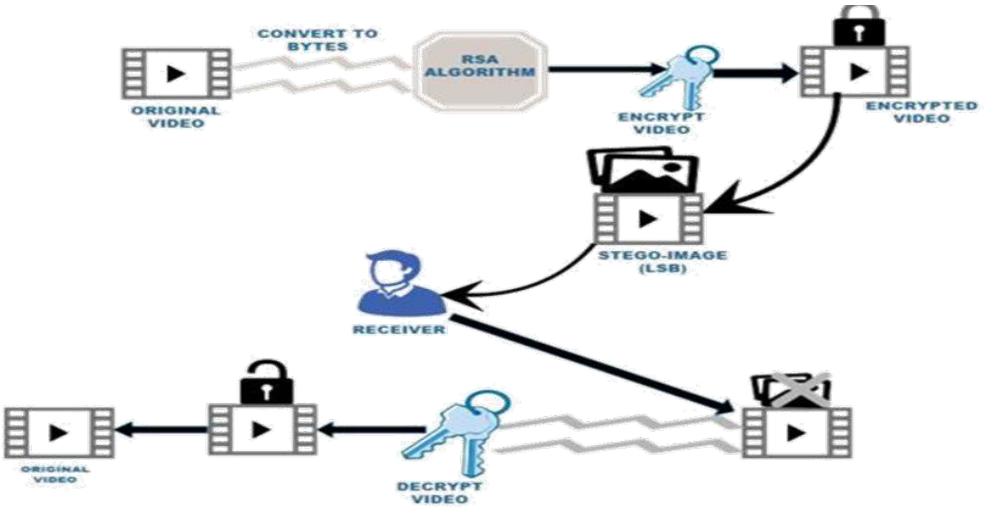

Figure 1: StegoVideo Architecture

Algorithm 1: StegoVideo Key Generation

Begin
For all video data V_t
Start
Generate a pair V_i and V_j, where $V_i \neq V_j$
Compute $V_n = V_i V_j$
Obtain the function $\rho(v_n) = (v_i - 1)(v_j - 1)$
Choose an integer m; such that $m > \rho(v_n); 1 < m < \rho(v_n)$
Compute the Keys for the video data V_k
$V_k = m^{-1} \bmod \rho(v_n)$
Generate public key $(V\ ideoP_i)$ such that $VideoP_i = m, V_n$
Generate private key $(V\ ideoP_j)$ such that $VideoP_j = V_K, V_n$
Stop
ProtectV_k, V_i, and V_n
End

Algorithm 2: StegoVideo Hybrid Process

Input: Private key $(VideoP_j)$, public key$(VideoP_i)$, secret message (S_i)
Output: Encrypted video V_e Stego-image $(Stego_i)$
Begin
For all video databases V_d
Start
Select video data $M_1, M_2, \ldots \ldots, M_n$ such that $M \in V_d$
Convert M_n to bytes
Verify $(VideoP_i)$ for video data M_n
If $M_n \in [0, V_n - 1]$
Obtain cipher text $(T_k = M_i^{V_k} \bmod V_n)$
Produce the encrypted video (V_e)
Obtain S_i and convert S_i to bits (S_b)
Select cover image (V_c) for each V_e and compute LSB
Embed S_b into V_e
Check if$V_e \equiv hidden$, otherwise repeat the process
Stop
Display the stego-image $Stego_i$
End

The second phase of the StegoVideo system is the hybrid process as represented in Algorithm 2. At this phase, the video data to be transmitted is converted into bytes and the algorithm verifies the public key generated in Algorithm 1. Once the public key is valid, the encrypted video data is generated using the public key as depicted in Lines 3-7 of Algorithm 2. To further protect the encrypted video, the system generates a secret message and transforms the message into strings of zeros (0) and ones (1). Additionally, a cover picture is selected and LSB bits are computed. Thereafter, the secret image bits are concealed in the cover picture. This procedure is repeated until all the video data are completely hidden as represented in Lines 8-12 of Algorithm 2. Once, the steganography process is achieved on the encrypted video, then a stego-image is generated which is transmitted to the receiver.

The last phase of the StegoVideo system is the decoding process; it involves the method of un-hiding the stego-images and decrypting video data as presented in Algorithm 3. The LSB operation is performed on the received information to separate the secret messages, cover images, and encrypted videos in the stego-images. Further, the algorithm will test if the retrieved encrypted video is complete and valid as shown in Lines 3-7 of Algorithm 3. Once, the complete encrypted video is retrieved, the private key is obtained using the procedures in Algorithm 1. The generated private key will be used to decrypt the video back to its initial state before encryption.

Algorithm 3: StegoVideo Decoding Process

Begin
For all $(Stego_i)$ transmitted to the recipient
Start
Obtain LSB for $(Stego_i)$
$\forall (Stego_i)$, Separate $(V_c), (S_i)$ and $(V_e) \in Stego_i$
$If\ (V_e) \rightarrow$ valid $\cap$ Complete, extract (V_e)
Generate $VideoP_j$using Algorithm1
Decrypt V_e with $VideoP_j$
Stop
Obtain original video data (M_n)
End

IMPLEMENTATION AND EVALUATION

The prototype of the StegoVideo system and the evaluation results are presented in this section. To implement the StegoVideo model, all the StegoVideo algorithms presented in Section 3 are converted to Java codes, and the system is evaluated using some performance metrics. The key generation Interface as shown in Figure 2 provides a graphic user interface (GUI) for the automatic generation of key pairs (public and private keys). The application also provides a GUI for the selection and encryption of video files as displayed in Figures 3 and 4. The implementation of the steganography is presented in Figures 5 and 6; the application allows image selection for the encrypted videos as shown in Figure 5. Figure 6 displays the result after embedding the encrypted video. The decoding process interface is given in Figure 7, the system provides a GUI decryption button to perform the decryption process.

Figure 2: Key Generation Interface

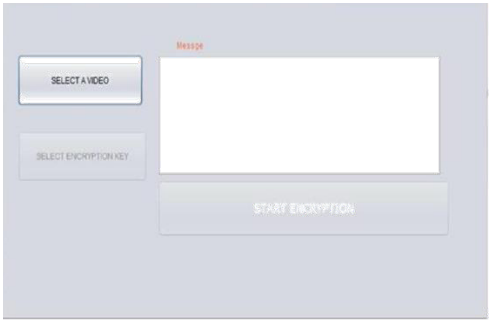

Figure 3: Video-File Selection Interface

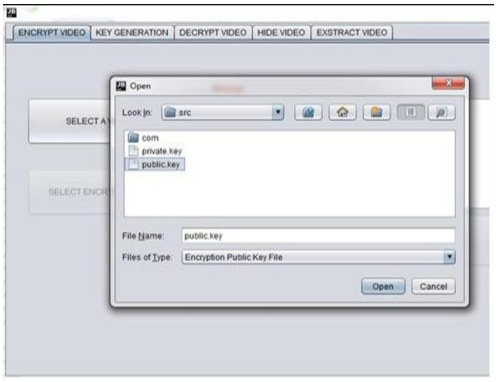

Figure 4: Video Encryption Interface

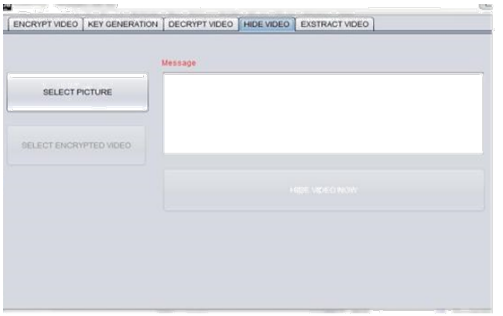

Figure 5: Image Selection for Steganography

Figure 6: Result after Embedding the Encrypted Video

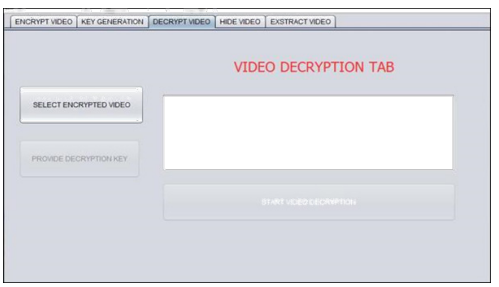

Figure 7: Decoding Process Interface

The performance of the StegoVideo system is tested on the RSA algorithm and steganography individually and hybrid process. The data for file size before and after encryption, encryption time, and decryption time is obtained as given in Table 1. Graphical representations of the results obtained are presented in Figures 8-9. After testing the performance of each technique individually, it was observed that the RSA algorithm retains the original size of the video after encryption is done. The evaluation analysis also revealed that the image in the steganography process increases in size after hiding the original video in it and the image quality as well remains the same. Through extensive evaluation, it was discovered that the size of the picture determines the video size that can be covered up. Furthermore, the experiment conducted when the two techniques are applied on the StegoVideo system showed that the increase in stego-image size is similar to the result obtained when tested with a single approach (either RSA or LSB). The experimental investigation revealed that when the encryption technique alone is applied to the StegoVideo system, the existence of the video can be easily detected by unknown users. Additionally, the StegoVideo evaluation results when tested with the steganography process only; showed low-level security because the video content could be extracted from the image. However, the StegoVideo system shows high-level security and retains the original size and quality of the video after decryption when tested with these two techniques which make the scheme suitable for live and pre-recorded video streaming applications.

Table 1: Performance Comparison

Video size(MB)	Encryption time (ms)	Video size after encryption(MB)	Decryption time (ms)
1.12	1040	1.12	1020
0.67	740	0.67	730
1.08	670	1.08	770
0.94	730	0.94	870
0.71	710	0.71	760

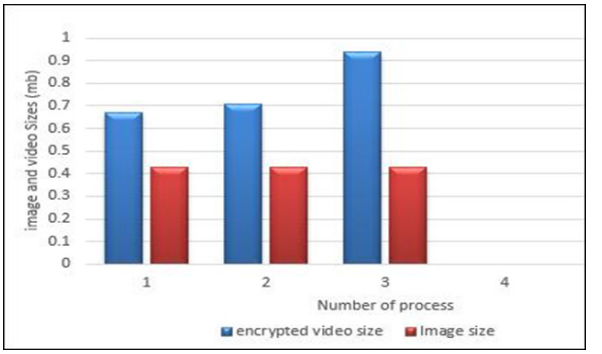

Figure 8: Stego-Image vs Encrypted Video

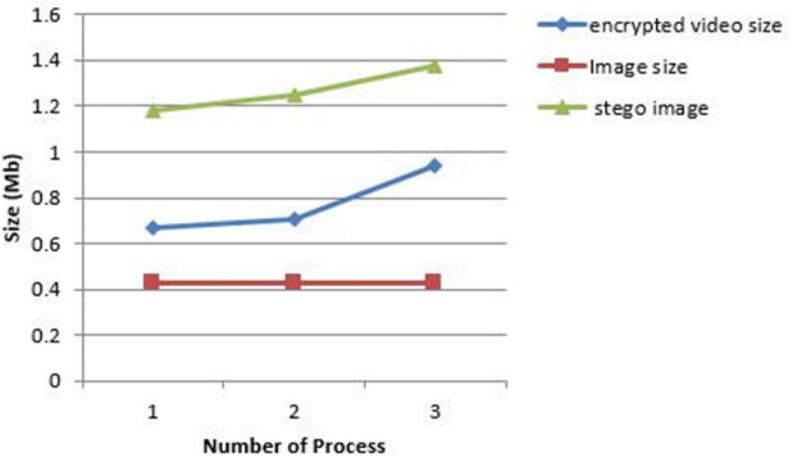

Figure 9: Image size, Encrypted video size, and Stego-image size

CONCLUSIONS

A hybrid framework for securing video data named "StegoVideo" is proposed in this research. The StegoVideo system adopts RSA encryption and LSB steganography to guarantee an undeniable level of security for video data transmitted in the network. The StegoVideo is implemented and evaluated using selected performance metrics. The evaluation results showed that StegoVideo is a strong and effective security framework suitable for dealing with sensitive or secretive video data. In addition, the experiment conducted on StegoVideo demonstrates that the video quality of the transmitted video is retained after decryption which makes it suitable for live streaming applications such as virtual learning, and virtual meetings. It is extremely important to state that the StegoVideo System has addressed the security issues associated with video streaming applications by protecting them from being accessed by unauthorized users or individuals. However, it was observed that the framework requires a lot of space to conceal the video in an image for the steganography cycle and the encryption process takes a longer processing time when dealing with huge videos. Subsequently, the StegoVideo framework can additionally be refined to decrease space for the image concealing process and minimize processing time.

REFERENCES

Abd-Elrahman, E., Boutabia, M., & Afifi, H. (2010). Video streaming security: reliable hash chain mechanism using redundancy codes. *In Proceedings of the 8th InternationalConference on Advances in Mobile Computing and Multimedia*, pp. 69-76.

Abdulla, A. A., Sellahewa, H., & Jassim, S. A. (2019). Improving embedding efficiency for digital steganography by exploiting similarities between secret and cover images. *Multimedia Tools and Applications*, 78, 17799-17823.

Akoum A, Moughrabi W. (2020) The implementation of hamming code using video steganography. *International Journal of Sciences: Basic and Applied Research*, 53(2):46- 58.

Alabdullah, B., Beloff, N., & White, M. (2021). E-ART: A new encryption algorithm based on the reflection of binary search tree. *Cryptography*, 5(1), 4.

Alhassan, S., Iddrisu, M. M., & Daabo, M. I. (2018). Perceptual video encryption via unit anti- diagonal matrix. *Appl. Math. Inf*. Sci, 12(5), 923-929.

Almadani, B., Alsaeedi, M., & Al-Roubaiey, A. (2016). QoS-aware scalable video streaming using data distribution service. *Multimedia Tools and Applications*, 75, 5841-5870.

Dalal, M., & Juneja, M. (2019). A robust and imperceptible steganography technique for SD and HD videos. *Multimedia Tools and Applications*, 78(5), 5769-5789.

Duan, X., Guo, D., Liu, N., Li, B., Gou, M., & Qin, C. (2020). A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network. *IEEE Access*, 8, 25777-25788.

Favale, T., Soro, F., Trevisan, M., Drago, I., & Mellia, M. (2020). Campus traffic and e- Learning during COVID-19 pandemic. *Computer networks*, 176, 107290.

Gutte, R. S., Chincholkar, Y. D., & Lahane, P. U. (2013). Steganography for two and three LSBs using extended substitution algorithm. ICTACT *Journal on communication technology*, 4(01), 685-690.

Gutub, A., & Al-Ghamdi, M. (2020). Hiding shares by multimedia image steganography for optimized counting-based secret sharing. *Multimedia Tools and Applications*, 79(11), 7951-7985.

Hamidouche, W., Farajallah, M., Sidaty, N., El Assad, S., & Deforges, O. (2017). Real-time selective video encryption based on the chaos system in scalable HEVCextension. Signal Processing: Image Communication, 58, 73-86.

Kumar, N., & Chaudhary, P. (2016). Implementation of modified RSA cryptosystem for data encryption and decryption based on n prime number and bit stuffing. *In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*, pp. 1-6.

Kurniawan, F., & Satrya, G. B. (2021). Future Identity Card Using Lattice-Based Cryptography and Steganography. *In Advances in Computer, Communication and Computational Sciences: Proceedings of IC4S 2019*, Springer, Singapore, pp. 45-56.

Liu, H. C., & Chen, W. (2020). Optical ghost cryptography and steganography. *Optics and Lasers in Engineering*, 130, 106094.

Manisha, S., & Sharmila, T. S. (2019). A two-level secure data hiding algorithm for video steganography. *Multidimensional Systems and Signal Processing*, 30, 529-542.

Mohsin, A. H., Zaidan, A. A., Zaidan, B. B., Mohammed, K. I., Albahri, O. S., Albahri, A. S., & Alsalem, M. A. (2021). PSO–Blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in decentralised hospitals intelligence architecture. *Multimedia tools and applications*, 80, 14137-14161.

Mondal, A., & Goswami, R. T. (2021). Enhanced Honeypot cryptographic scheme and privacy preservation for an effective prediction in cloud security. *Microprocessors and Microsystems*, 81, 103719.

Nyo, H. L., & Oo, A. W. (2019). Secure data transmission of video steganography using Arnold scrambling and DWT. *International Journal of Computer Network and Information Security*, 9(6), 45.

Pramanik, S., Bandyopadhyay, S. K., & Ghosh, R. (2020). Signature image hiding in color image using steganography and cryptography based on digital signature concepts. *In 2020 2nd International Conference on Innovative Mechanisms for Industry Applications, IEEE*, pp. 665-669.

Rabah, K. (2005). Theory and implementation of data encryption standard: A review. *Information Technology Journal*, 4(4), 307-325.

Roselinkiruba, R., & Hemalatha, R. (2023). Secure video steganography using key frame and region selection technique. International Journal of Information Technology, 15(3), 1299-1308.

Sam, D., Nithya, K., Kanmani, S. D., Sheeba, A., Ebenezer, A. S., Maheswari, B. U., & Amesh, J. D. (2023). Survey of risks and threats in online learning applications. *In Secure Data Management for Online Learning Applications*, CRC Press, pp. 31-47

Sengupta, A., & Rathor, M. (2020). Structural obfuscation and crypto-steganography-based secured JPEG compression hardware for medical imaging systems. *IEEE Access*, 8, 6543-6565.

Seufert, M., Casas, P., Wehner, N., Gang, L., & Li, K. (2019, February). Stream-based machine learning for real-time QoE analysis of encrypted video streaming traffic. *In 2019 22nd Conference on*

innovation in clouds, internet and networks and workshops (ICIN), IEEE, pp. 76-81.

Shanthakumari, R., & Malliga, S. (2020). Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm. *Multimedia Tools and Applications*, 79(5), 3975-3991.

Soliman, N. F., Khalil, M. I., Algarni, A. D., Ismail, S., Marzouk, R., & El-Shafai, W. (2021). Efficient HEVC steganography approach based on audio compression and encryption in QFFT domain for secure multimedia communication. *Multimedia Tools and Applications,* 80, 4789-4823.

Song, X. H., Wang, H. Q., Venegas-Andraca, S. E., & Abd El-Latif, A. A. (2020). Quantum video encryption based on qubit-planes controlled-XOR operations and improved logistic map. *Physica A: Statistical Mechanics and its Applications*, 537, 122660.

Suresh, M., & Sam, I. S. (2020). Optimal wavelet transform using Oppositional Grey Wolf Optimization for video steganography. *Multimedia Tools and Applications,* 79, 27023- 27037.

Tarun, M. V. S., Rao, K. V., Mahesh, M. N., Srikanth, N., & Reddy, M. (2020). Digital video steganography using LSB technique. *Red*, 100111(11101000), 11001001.

Wahab, O. F. A., Khalaf, A. A., Hussein, A. I., & Hamed, H. F. (2021). Hiding data using efficient combination of RSA cryptography, and compression steganography techniques. *IEEE Access,* 9, 31805-31815.

Xu, D. (2019). Commutative encryption and data hiding in HEVC video compression. *IEEE Access,* 7, 66028-66041.

Yaacoub, J. P., Noura, H., Salman, O., & Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things,* 11, 10