Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

# An Efficient Enhanced Full Homomorphic Encryption For Securing Video In Cloud Environment

**Geetha N** ( geetha.researchscholar@gmail.com )
Alagappa University Faculty of Science https://orcid.org/0000-0002-4674-2080
**Mahesh K**
Alagappa University Faculty of Science

**Research Article**

**Keywords:** Cloud computing, Key generation, Fully Homomorphic Encryption, Video encryption,

**Posted Date:** May 26th, 2021

**DOI:** https://doi.org/10.21203/rs.3.rs-554651/v1

**License:** This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

# An Efficient Enhanced Full Homomorphic Encryption For Securing Video In Cloud Environment

N.Geetha[1]*, Dr.K.Mahesh[2]
[1]Ph.D Scholar, Department of Computer Applications, Alagappa University, Karaikudi, Tamilnadu.
Email: geetha.researchscholar@gmail.com
[2]Professor, Department of Computer Applications, Alagappa University, Karaikudi, Tamilnadu.

**Abstract**

At present days, exponential growth in the transmission of multimedia data takes place due to a significant rise in network bandwidth and video image compression technologies. However, the transmission of videos over wireless channels often brings an unseen risk that sensitive video details might be corrupted and distributed in an illegal way. So, the security of video transmission has become a hot research topic. Several encryption models have been presented in the literature, yet, it is believed that the performance of encryption process can be further improved. In this perspective, an efficient novel video encryption technique is presented using an enhanced variant of Fully Homomorphic Encryption (FHE) model called as EFHE model. By the hybridization of Ducas and Micciancio (DM) with the FHE model presented by Gentry, Sahai, and Waters (GSW), matrix operations vector additions are properly employed in the proposed EFHE model. In addition, a new key generation scheme to increase the fastness of the encryption process. The EFHE model is designed and placed on a cloud environment which leads to reduced cloud user's communication and computation complexity. It is ensured that the presented EFHE model is highly efficient and secure over the compared methods.

**Keywords:** Cloud computing, Key generation, Fully Homomorphic Encryption, Video encryption,

## 1. Introduction

Recently, due to the fast growth of internet and big data methodologies [1–5], cloud computing (CC) becomes a most significant technology. Here, CC offers more opportunities based on trading with on-demand solution that helps several other firms to consume the services provided by cloud in terms of infrastructure to perform different activities like data maintenance, business development as well as service organization [6]. Additionally, CC offers different types of cloud services to each user. Generally, the video services provided by cloud provisioner have enhanced the customer experience [7]. Therefore, the video which has been stored in cloud comprises of typical features such as higher volume, maximum redundancy, and rapid real-time necessity. In case of compressed video, it requires some parameters like data location indexing as well as controllable coding rate. But, CC is assumed to be suspicious about the security measures where it is capable of ensuring security of video in cloud. It can also be stated that, users could not be depended on cloud service providers (CSP) for complete trust [8]. Initially, when it comes to multitenant resource distributing platform, the user provides the overview of video that might be malfunctioned, released and unauthenticated data which will be scattered over CSP. Alternatively, a threat would be existed by third party access since the virtual machines (VM) does not protect the isolated data. Followed by, the information and operations present in CC would be in

the form of scattered way where the data comes under various groups which may be distributed along with a guarantee of integrity and non-leakage [9]. Based on these functions, the features of video data encryption have to follow 5 characteristics namely, Security, Compression Ratio (CR), Real-Time, Data Format Invariability and Data Operability.

Security is the basic ingredient for encrypting a data. It is common that the security measure is higher when compared to directly obtaining the password where cryptosystem is more secured. As the video data is considered to be normal binary information, the traditional key might be applied while encrypting video. Also, massive amount of video information tends to raise the level of complexity while code-breakers imminently compute more number of decoding function on the data which has been encrypted. Hence, rapid and common encrypting technique could be employed to assure the security.

CR is the process of retaining similar data without any modification process, i.e., the data remains same before and after encoding process. This process is said to compression rate invariability. While encrypting the data with the help of compression rate, invariability cannot alter the external memory space where transmission ration is retained with the same value. Real-Time plays a significant role in real-time communication process as well as it uses the video information. Also, the application of encryption and decryption techniques does not produce more latency. Hence, the real-time transmission can be effective using rapid encryption and decryption techniques.

Data Format Invariability defines that the template of a video data has not been modified either by encryption or decryption process. The above processes tend to emerge several merits. The most significant factor is to create timing for possible video data that allows the support of addition, deletion, copy, paste function of data.

Data Operability is essential for the purpose of direct performance in encrypted information rather to determine the cumbersome process for decryption as well as encryption. Some of the processes involved here is rate control, image block clipping, and so on. Any operation with minimum process might be operated if the data undergoes encryption which is comprised with data operability. In earlier times, various encryption models have been employed for MPEG videos [10]. The main of an algorithm is to assure the real-time video streaming as well as display operation where few techniques ensure that CR remains the same. Also, few parameters like compatibility, operability, abnormality [11], and routing [12, 13] which have been reported in alternate techniques. According to the variations among encryption and compression coding operation, the existing models are classified into various segments that are provided as direct encryption algorithm, Selective encryption algorithm and Encryption algorithm.

In direct encryption algorithm, video data is assumed to be normal information that can be encrypted directly without any interrupts. Thus, a technique which comes under this division does not pose compatibility. Then, selective encryption algorithm consists of partial video data that is encrypted in a selective manner; also, it is compatible in nature. Next, encryption algorithm is integrated with compression process. Some of the algorithms that comes under in this division concatenates the encryption process, compression and encoding process in group which tends to grasp the characteristics of being compressive, compatible, as well as operable. This paper has been focused on the study on the Homomorphic Encryption (HE). The client is capable of

validating the probity of information as well as to support the overall validation and data dynamics. By applying the HE tags, the bandwidth requirement could be minimized to a greater extent that is mainly used in video data encrypting observation. Subsequently, the presented model as well as induced services has been applied on cloud system that decreases the interaction among cloud user as well as processing overload. Hence, it is possible by security examining and computation analysis along with executed outcomes.

This paper presents a new video encryption technique using an enhanced variant of Fully Homomorphic Encryption (FHE) model called as EFHE model. By the hybridization of Ducas and Micciancio (DM) with the FHE model presented by Gentry, Sahai, and Waters (GSW), the matrix operations vector additions are properly employed in the proposed EFHE model. In addition, a new key generation scheme to increase the fastness of the encryption process. The inclusion of advanced key generation process shows the novelty of the work. The EFHE model is designed and placed on a cloud environment which leads to reduced cloud user's communication and computation complexity.

**2. Related work**

In general, resource monitoring is a crucial part in resource managing process from cloud environment [14]. This is helpful in providing fundamental units for allocating resources, scheduling task as well as load balancing [15]. AS the CC platform is composed with some features as transparent virtualization and resource flexibility where there is no possibility in applying traditional approach for protecting the data security from cloud environment. In addition, few more characteristics like collection, transmission, memory, and computation for massive amount of checked data that leads to increase the cost of these processes. Here, cryptographic protocol plays an important role in several other security techniques [16]. It is mainly applied in various domains like financial trading, social network, real-time controlling, as well as data management. Traditional cryptographic protocols are generally applied with multiple participants, which are the most trusted groups or unauthenticated users. Generally, the protocols that are not secured are capable of adopting complete HE system. Several applications of HE is assumed to be in secured multiparty processing. The complete HE enables many processes to take place in absence of private key. As a result, the computation of sensitive information along with the encryption should be provided which leads to solve the issues of data security as well as other challenging factors [17].

The HE technique is assumed to be data obfuscation algorithm in coding obfuscation [18]. Data present in a program is composed with characters and numerical values. But, applying HE system for numbers is inefficient. Furthermore, the efficiency of the program would be reduced once the code is obfuscated. Also, Fourier transform helps in reducing the computational cost as well as length of cipher video. This process tends to enhance the effectiveness of the program at the time of security ensuring. Here, data obfuscation within code obfuscation is comprised with polynomial obfuscation, data transformation obfuscation, and so on. A major benefit expelled from this technique is that data could be represented while encrypting and decrypting the information. The HE method is performed internally in the absence of decryption operation. Since there is a raise in demand for data security is most essential in the application of CC as well as e-commerce, a study on HE techniques has been performed [18]. From the above functions, it is noted that HE can be employed in CC along with a number of operations which satisfies several addition and minimum multiplications are applicable in privacy-preserving clouds. Consequently, Standard deviation (SD) is in need of single multiplication as well

as predictive analyzing schemes like logistic regression (LR) acquires only minimum multiplication process. From HE techniques [19], few models such as RSA convince multiple homomorphism [20] and alternate models satisfy the additional homomorphism [21]. Also, FHE is enabled with the feature of finite homomorphic functions which attains maximum efficiency with smaller size of cipher video.

While applying protocol relied on homomorphic method in order to verify the potential of cloud video data, the network bandwidth resources has been utilized in a minimum amount during the implementation process. It is due to the servers are required to transmit the integrity proof for clients with no returning of original video files. Additionally, it allows the customers to predict the corrupted videos that are recorded in the cloud that tends to minimize the time consumption to recover the data [20]. The data integrity checking protocol depends upon the homomorphic scheme that often consists of several integer exponential functions on elliptic curve. The above factor leads to increase the processing speed. In particular, the users are provided with lower computation [22], which consumes more time of interval in homomorphic tags that has to be produced for video file blocks in prior to upload the video files to CC platform. To determine the lifetime of integrity evidence is in need of maximum duration. Though the cloud providers are embedded with effective computation ability, it conserves more amount of resources during the process of verifying integrity for existing customers respectively.

A novel leveled FHE scheme, called GSW is proposed by Gentry, Sahai and Waters [23]. It depends upon the approximate eigenvectors of matrices. The cipher text in GSW are square matrix, and homomorphic additions and multiplications are just matrix additions and multiplications, correspondingly. So, cipher text dimension continuously retains constant and key switching is unnecessary. Ducas and Micciancio (DM) [24] is developed by the concepts of ciphertext matrix operations in the FHE scheme proposed by GSW. The presented DM model is theoretically modest compared to several FHE models, while suffering from low efficiency.Cheng et al. [25] presented a novel four-dimensional (4-D) hyperchaotic technique for protecting the data privacy for further improving the secrecy of the video encryption. The symmetric encryption necessitates that the matching key is utilized for encryption and decoding. Here, the symmetry model is applied for protecting the privacy of the video data owing to the massive quantity of video encrypted data. In [26], a novel end to end encryption technique called SmartEdge, for a smart city application by the execution of the computationally complex processes at the network edge and cloud data centers. By the use of a lightweight symmetric encryption technique, a secure connection amongst the smart core devices for multimedia streaming towards the recorded and confirmed edge devices.

## 3. Proposed system

### 3.1. The GSW Scheme

The GSW approach has been built on the basis of adjacent eigenvectors which has been obtained from matrices. The GSW scheme is depicted in Fig. 1. The homomorphic functions within GSW are only cipher video matrix operations. Therefore, GSW is assumed to be natural as well as concise when compared with existing LWE-based FHE techniques that is in need of key switching. The major techniques present in GSW have been computed in the following:

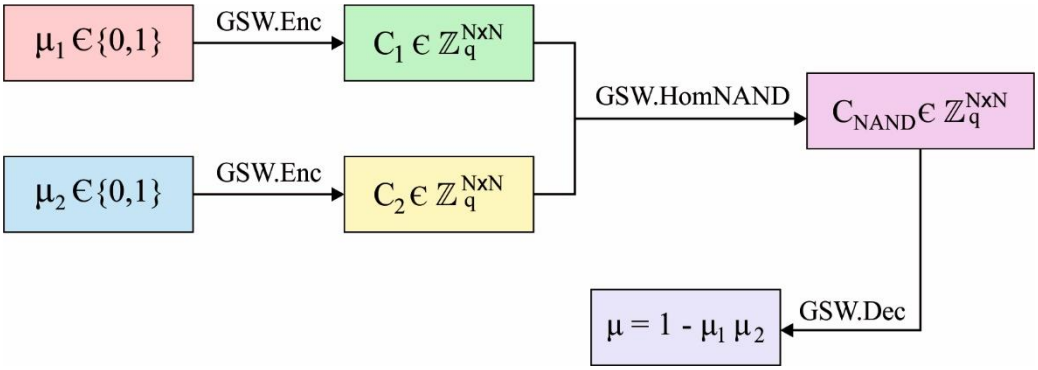


**Fig. 1.** Flowchart of GSW scheme

**(i) GSW.KeyGen($\lambda, L$):** $\lambda, L$ implies the security measure as well as multiplicative depth. The Cipher video dimension $n = n(\lambda, L)$, modulus $q = q(\lambda, L)$, and noise distribution $\chi = \chi(\lambda, L)$ has ensured the security level for $\lambda$. Alternatively, let $m = O(n \log q)$, $l = \lfloor \log q \rfloor + 1, N = (n+1)l$, and parameter as set params$= (n, q, \chi, m)$. Then, Sample $t \leftarrow \mathbb{Z}_q^n$, let $s = (1, -t) \in \mathbb{Z}_q^{n+1}$, as well as simulation outcome of secret key $sk = v = PT(s)$ . Sample $B \leftarrow \mathbb{Z}_q^{m \times n}, e \leftarrow \chi^m$, let $b = B \cdot t + e, A = [b \| B]$, and final outcome of public key$pk = A$.

**(ii) GSW.Enc(params, pk, μ):** The plain video $\mu \in \mathbb{Z}_q$, sample $R \leftarrow \{0,1\}^{N \times m}$; output cipher video:

$$C = FL\left(\mu \cdot I_N + BD(R \cdot A)\right) \in \mathbb{Z}_q^{N \times N} \quad (1)$$

where $I_N$ is the N-dimensional identity matrix.

**(iii) GSW.HomNAND($C_l, C_2$):** from input cipher video pair $C_1, C_2 \in \mathbb{Z}_q^{N \times N}$, outcome cipher video

$$C_{NAND} = FL(I_N - C_1 C_2) \quad (2)$$

Finally, the simulation outcome of homomorphic NAND operation as,$C_{NAND}$ convince the upcoming features:

$$C_{NAND} \cdot v = (1 - \mu_1 \mu_2)v - \mu_2 e_1 - C_1 e_2 \quad (3)$$

where $\mu_1$, $\mu_2$ denotes the plain video present in $C_1$, $C_2$, and $e_1$, $e_2$ refers the neighbouring cipher video noises, $B_0$indicates the upper bound of noise magnitudes from $C_1, C_2$, which is the upper bound of $l_\infty$ in terms of $e_1$,$e_2$. It is the fact that$\max\{\|e_1\|_\infty, \|e_2\|_\infty\} < B_0$. Generally,$C_1$, $C_2 \in \{0,1\}^{N \times N}$ that results in flatten performance. Since $\mu_2 \in \{0,1\}$, noise in $C_{NAND}$ has been upper bounded through $(N+1)B_0$, as depicted in (3).

### 3.2. The DM Scheme

Here, DM is considered as FHE model which is relied on LWE symmetric encryption method [27]. The homomorphic functions of DM that has additional cipher video. The DM scheme is illustrated in Fig. 2.

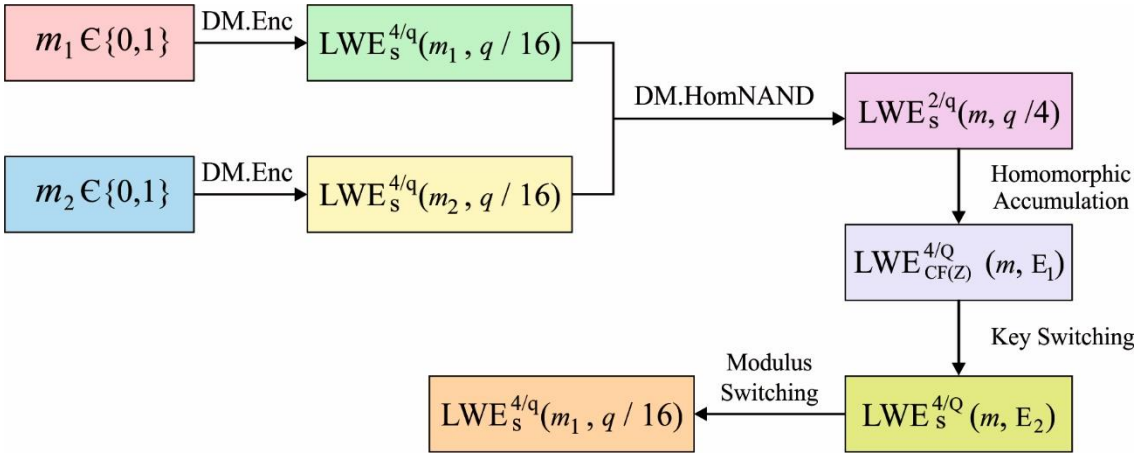


**Fig. 2.** Flowchart of DM scheme

The most significant technique of DM has been illustrated by the following properties:

**(i) DM.KeyGen (λ):** λ represents the security features. Also, the integer $t \geq 2$ is said to be plain video modulus. Cipher video dimension $n = n(\lambda)$, modulus$q = q(\lambda)$, as well as cipher video noise distribution $\chi = \chi(\lambda)$ has to ensure the trust phase of λ, $x < q/2t$ for different $x \leftarrow \chi$. Let params signify the parameter set $\text{params} = (n, q, t, \chi)$ . Therefore, key is tested from

$$\mathbb{Z}_q^n : \frac{pk}{sk} \leftarrow \mathbb{Z}_q^n. \tag{4}$$

**(ii) DM.Enc(m, pk, params):** The plain video and cipher video spaces are denoted as $\mathbb{Z}_r, \mathbb{Z}_q$. Sample $a \leftarrow \mathbb{Z}_q^n, e \leftarrow \chi$, for input plain video $m \in \mathbb{Z}_r$, as well as final resultant cipher video:

$$LWE_s^{t/q}(m) = \left(a, a \cdot s + \frac{mq}{t} + e\right) \in \mathbb{Z}_q^{n+1} \tag{5}$$

**(iii) DM.HomNAND**$\left((\mathbf{a_l}, \mathbf{b_1}), (\mathbf{a_2}, \mathbf{b_2})\right)$: Based on input cipher videos $c_i = (a_i, b_i)$, $i \in \{1,2\}$ and $c_i \in LWE_s^{4/q}(m_i, q/16)$ undergoes encryption with the plain video $m_j$, as outcome as $c = (a, b)LWE_s^{2/q}(1 - m_l m_2, q/4)$ . Specifically,

$$(a, b) = \left(-a_1 - a_2, \frac{5}{8}q - b_1 - b_2\right) \tag{6}$$

The cipher video $(a, b)$ is assumed as cipher video which is obtained from $1 - m_l m_2$ along with noise magnitude which is lower than $q/4$, that ensures the result to be accurate decryption. The homomorphic NAND functions in DM have been completed under the application of some additional features among cipher video which is easier and rapid when compared with tensor operation in existing techniques. But, cipher video magnitude has the value of $q/4$ once the homomorphic operation is performed once again. Followed by, cipher video has not been decrypted exactly. When all homomorphic operation gets completed, the cipher video should be regained in order to maintain the noise magnitude in a minimum value.

The effective cipher video refreshing technique is operated on the basis of Ring-GSW that is presented in DM to minimize the noise present in cipher video. The refreshing model is composed with, cipher video $(a, b) \in \mathrm{LWE}_s^{2/q}(m, q/4)$ as well as refreshing key $K_{rf}$ is assumed to be input, and base $B_r$ has been applied for encoding the cipher video $(a, b)$ . Therefore, $K_{rf}$ is comprised with the cipher video as given below:

$$K_{i,c,j} = E\left(cs_i B_r^j \bmod q\right) \tag{7},$$

$$c \in \{0, , B_r - 1\}, j = 0,, d_r - 1, i = 1,, n$$

where $d_r = \lceil \log_{B_r} q \rceil$ and $E(\cdot)$ implies the encryption technique for cipher video refreshing algorithm. The cipher video refreshing method is illustrated in Algorithm 1, and Init $(\cdot)$ and Incr $(\cdot)$ represent initializing as well as homomorphic summation of accumulator ACC, correspondingly. The ACC can be declared as encrypting model of $b + q/4$. If the main loop present in Algorithm 1 gets completes then, the provided plain video $\nu$ of the accumulator satisfies

$$\nu - \frac{q}{4} = b + \sum_{i,j} a_{i,j}\, s_i B_r^j = b + \sum_i s_i \sum_j B_r^j\, a_{i,j} \quad = b - \sum_i a_i S_i\, s_j = \frac{q}{2} m + e \tag{8}$$

where $e$ indicates the presence of noise in input cipher video $(a, b)$ . Since $|e| < q/4$, it is noted that $0 < \nu < q/2$ If $m = 0$ and $q/2 < \nu < q$ when $m = 1$. Besides, extraction of most significant bit (msb) present in $\nu$ is capable of producing original video $m$ respectively.

When msb Extract process has been with accumulator ACC, with a switching key $K_{ks}$ and a sample vector of $t = -\sum_{i=0}^{q/2-1} C\, F(Y^i)$, that is obtained as input. In addition, $Y = X^{2N/q}$, and $z \in R$ is termed as secret key which has been applied as cipher video refreshing algorithm.

Also, the cipher video $c$ could be denoted as

$$c = (a, b_0 + u) = \left(a \cdot C\Gamma(z) + t \cdot e + 2u.\, \mathrm{msb}\,(\nu)\right) \tag{9}$$

where $a = t^t$ . $\mathrm{ACR}(a)$, $[a, b']$ is a second row of ACC and $u = \lceil Q/2t \rceil$ or $\lfloor Q/2t \rfloor$. Let $u \approx Q/2t, c$ is the encryption of $\mathrm{msb}(\nu) = m$. Hence, $c \in \mathrm{LWE}_{C\Gamma(z)}^{r/Q}\left(\mathrm{msb}(\nu)\right)$ . Once the key and modulus switching has been completed and $c$ is transmitted to a cipher video with the help of under key $s$ modulo $q$. With the proper parameter setting, noise magnitude of refreshed cipher video might be lesser than $q/16$, that tends to proceed with further operations.

### 3.3. Efficient FHE Scheme

According to GSW and DM methods, it mainly concentrates in overly cipher video refreshing's among DM, a novel fully homomorphic encryption (FHE) technique has been presented (NHE) to attain maximum efficiency. The cipher video matrix functions of GSW and cipher video vector additions of DM have been applied in this paper. The major benefits of GSW and DM are simple and easy that is emerged in this technique. The overall process is illustrated in Fig. 3. Once the video needs to be accessed from the cloud by the trusted party, the data will be encrypted by the use of enhanced version of FHE (EFHE) scheme. In EFHE, the hybridization of DM

with the FHE model presented GSW takes place. When the other participants need to access the data from the cloud, the cloud service application executes the data processing algorithm and then sends the encrypted video by the use of FEHE model. Also, it has the combination of merits of effective homomorphic process in DM along with the advantage of gradual development in noise magnitude of GSW respectively.

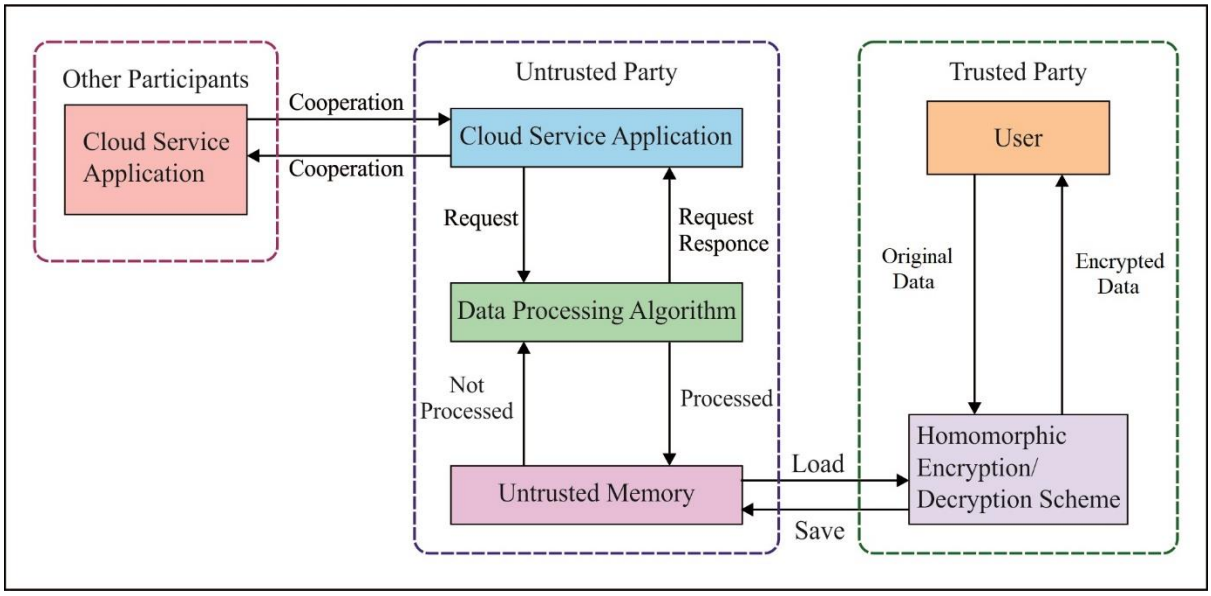


**Fig. 3.** Working process of EFHE method

**(i) NHE.KeyGen (λ):** Here λ represents the security attribute. Modulus $q = q(\lambda) = 2^k (k \in \mathbb{Z}^+)$, dimension $n = n(\lambda)$, and cipher video noise distribution $\chi = \chi(\lambda)$ has been combined to enhance the level of security λ. Simultaneously, χ referred as discrete Gaussian distribution across the integers including zero mean as well as SD σ. Suppose the params implies the parameter set as $(n, q, \chi)$, and $l = \log q + 1, N = (n+1)l$ correspondingly. The sample $t \leftarrow \mathbb{Z}_q^n, s = (1, -t) \in \mathbb{Z}_q^{n+1}$; final secret key $sk = v = PT(s) \in \mathbb{Z}_q^N$. Sample $B \leftarrow \mathbb{Z}_q^{N \times n}, e \leftarrow \chi^N$, let $b = Bt + e, A = [b \parallel B]$, as well as output of public key $pk = A$.

**(ii) NHE.Enc$(m, pk)$:** The input plain video $m \in \{0, 1\}$, and output cipher video

$$C = FL\left(mI_N + BD(A)\right) \in \mathbb{Z}_q^{N \times N} \tag{10}$$

**(iii) NHE. HomNAND$(C_l, C_2)$:** the input cipher videos $C_1, C_2 \in \mathbb{Z}_q^{N \times N}$ has the encryption of $m_1, m_2 \in \{0,1\}$. All cipher video is comprised with interior parameter level which denotes the count of homomorphic process. Level of different cipher video could be 0 from initial stage as well as to improve the value by 1 for all homomorohic function. Here, $C_1, C_2$ such that $C_1 = C_2.level = 0$, homomorphic NAND operation might be computed below:

$$C' = FL(I_N - C_l C_2) \tag{11}$$

Followed by, the $(l-2)$-th row can be obtained from $C'$ since the cipher video $c' \in \mathbb{Z}_q^N$ for upcoming homomorphic NAND process. The $c'.level = 1$. Pair of cipher videos $c_1', c_2' \in \mathbb{Z}_q^N$ in the form of $c_1'.level = c_2'.level = 1$, for which homomorphic NAND is processed as follows:

$$CNAND = \Gamma L(-c_1' - c_2' + c_0) \in \{0,1\}^N \tag{12}$$

where $c_0$ resembles an auxiliary vector as $c_O = BD((5q/8,0)) \in \{0,1\}^N$. The homomorphic mechanism of (18) and (19) is relied on the basis of cipher video matrix present in GSW as well as cipher video vector summation in DM.

**(iv)NHE.KeySwitch($c_{NAND}, K_{ks}$):** The switching key $K_{ks}$ is comprised with upcoming cipher videos: $k_{\iota,c} \in LWE_s^{q/q}(cv_i)$, $i = 1, \dots, N, c \in \{0, 1\}$, where $s' \leftarrow \{0,1\}^{n'}$ shows novel secret key. Based on input cipher video $c_{NAND}$ as well as switching key $K_{ks}$, such that final outcome cipher video

$$c'_{NAND=} \sum_i k_{\iota,c_i} \in \mathbb{Z}_q^{n'+1} \tag{13}$$

The above cipher video $c'_N$ AND is known to be cipher video from new secret key $s'$ by the replacement of v.

**(v) NHE.ModSwitch($c'_{NAND}$):** According to input cipher video $c'_{NAND}$, the output cipher video

$$c''_{NAND=} \left\lfloor \frac{q'}{q} c'^1_{NAND} \right\rceil \in \mathbb{Z}_{q'}^{n'+1} \tag{14}$$

where $q' = 2^{k'}(k' \in \mathbb{Z}^+)$ and $q' < q.c''_{NAND}$ indicates the result cipher video when 2 homomorphic NAND operations has been conducted. Then, modulus of $c''_{NAND}$ has been converted from q to $q'$. Therefore, dimension and modulus of $c''_{NAND}$ are fixed as similar to the cipher videos present in DM.

**NHE**. Key Switch tend to add the sum of $(n'+1)$-dimensional vectors, and NHE. Mod Switch refers the rounding for all coefficients from single vector. The technique is comprised with simple operations that have no important effect on simplicity of corresponding framework. $HomNAND_{DM}$ represents the models in Eqs. (10) and (11).

### 3.4. The key generation algorithm

A novel key generation technique has been presented to manage the limit of circuit depth. The centre point of this model could be defined in the following. The bound of evaluation circuit depth $d$ is fixed, as well as to determine the $r_{Dec} := (n\gamma)^{2^d}$. To attain the simplicity, set $r_{Enc} \leq n$ and choose $\lambda_1, \lambda_2, \dots, \lambda_n$ in a random manner, $s.t. 2r_{Dec} \leq \lambda_i$, to create the eigen values of matrix $B_\lambda$ respectively. On the other hand, the Gershgorin circle theorem states, to build as random matrix $A_{r\mathfrak{B}dom}$ like $a_{ij} \in [-(\lambda_{mm} - 2r_{Dec})/(n-1), (\lambda_{mm} - 2r_{Dec})/(n-1)]$. Additionally, primary matrix $B_p = B_\lambda + A_{random}$. is presented. Based on the correlation of bound of evaluation circuit depth as well as eigen values of matrix, the bound of evaluation circuit depth is greater than $d$ [28]. Alternatively, the secret key $B_J^{sk}$ has been determined with respective to $B_p$. At last, the value of HNF of $B_J^{sk}$, is computed as well as the simulation outcome as public key $B_J^{pk} = HNF(B_J^{sk})$ respectively. it can be fixed as $r_{Dec} := (n\gamma)^{2^d}$. When $r_{Enc} \leq n$, then

$$d \leq lg \frac{lgr_{Dec}}{lg(\gamma r_{Enc})} \leq lg \frac{lgr_{Dec}}{lg(\gamma n)} \tag{15}$$

then,

$$2^d \leq \frac{1gr_{Dec}}{1g(\gamma n)} \tag{16}$$

and

$$r_{Dec} \geq (\gamma n)^{2^d} \tag{17}$$

where $r_{Dec} := (n\gamma)^{2^d}$. The parameters involved are $n$: dimension of the lattice, $a_{ij}$: components of matrix $A_{random}$, $\varepsilon$: the threshold of $\delta_{orth-defect}$ and $d$: the upper bound of the evaluation circuit depth. Hence, key generation algorithm could be defined as follows.

**Input:** $d$ the upper bound of evaluation circuit depth.

**Step 1** Determine $r_{Dec} := (n\gamma)^{2^d}$ for $r := \{2, \sup \|uv\|/\|u\|\|v\| \neq 0$

**Step 2** Choose $\lambda_1, \lambda_2, \dots, \lambda_n$ arbitrarily s.t. $2r_{Dec} \leq \lambda_i$.

**Step 3** Produce an eigen value matrix $B_\lambda = [^{\lambda_1}\lambda_2 \cdots \lambda_n)$ , where empty positions are zero.

**Step 4** Choose a random matrix $A_{random}$ like

$$a_{ij} \in [-(\lambda_{mm} - 2r_{Dec})/(n-1), (\lambda_{mm} - 2r_{Dec})/(n-1)].$$

**Step 5** Determine $B_p = B_\lambda + A_{random}$

**Step 6** Generate the secret key $B_J^{sk} = B_p$.

**Step 7** Initiate the subroutine Gen $pk$.

Subroutine Gen $pk$:

**Input:** $B_J^{sk}$;

**Output:** $B_J^{pk}$

**Step 1** Calculate the $\delta_{orth-defect}(B_J^{sk})$ , if $\delta_{orth-defect}(B_J^{sk}) \geq 1 + \varepsilon$, continue; else, go to Step 3.

**Step 2** Calculate $B_J^{sk} = M_{rot_i}(v) B_J^{sk} M_{rot_i}^{-1}(v)$ in the form of $v = (1,0, \dots \dots 0)^T$ as subscript $i$ is chosen in a random manner from the set $\{1,2, \dots, n-1\}$ then, return to Step1.

**Step 3** Calculate $B_J^{pk} = HNF(B_J^{sk})$ .

**4. Performance Validation**

The proposed EFHE model is validated against a set of five benchmark videos namely Opening Ceremony, Soccer, Foreman, Football and Flowers [29]. The dimension of the Opening Ceremony and Soccer are 720x480 whereas the 312x288 is the dimension of Foreman, Football and Flowers dataset. In addition, the results are validated in terms of PSNR, SSIM, computation complexity, bit rate, and brute force attack analysis. For

comparison purposes, Energy-Aware Encryption (EAE) and Extended selective encryption (ESE) are employed [30].

### 4.1. PSNR and SSIM analysis

Table 1 shows the results offered by the EFHE model interms of PSNR and SSIM. Fig. 4 examines the video encryption performance of the FEHE model interms of PSNR. On measuring the results interms of PSNR, it is noted that maximum PSNR value of 13.36dB is offered by the EFHE model whereas lower PSNR values of 10.16dB and 9.12dB has been offered by the EAE and ESE models under the opening ceremony dataset. On measuring the results interms of PSNR, it is noted that maximum PSNR value of 14.62dB is offered by the EFHE model whereas lower PSNR values of 12.90dB and 12.44dB has been offered by the EAE and ESE models under the Soccer dataset.

**Table 1** Performance analysis of proposed with state of art methods in terms of PSNR and SSIM

| **Videos** | **PSNR** | | | **SSIM** | | |
|---|---|---|---|---|---|---|
| | **Proposed** | **EAE** | **ESE** | **Proposed** | **EAE** | **ESE** |
| **Opening Ceremony** | 13.36 | 10.16 | 09.12 | 0.298 | 0.265 | 0.216 |
| **Soccer** | 14.62 | 12.90 | 12.44 | 0.467 | 0.410 | 0.316 |
| **Fore man** | 15.49 | 13.87 | 11.71 | 0.432 | 0.379 | 0.325 |
| **Football** | 12.66 | 10.44 | 10.32 | 0.374 | 0.313 | 0.214 |
| **Flowers** | 11.54 | 09.46 | 09.31 | 0.380 | 0.295 | 0.212 |

On measuring the results interms of PSNR, it is noted that maximum PSNR value of 15.49dB is offered by the EFHE model whereas lower PSNR values of 13.87dB and 11.71dB has been offered by the EAE and ESE models under the Fore man dataset. On measuring the results interms of PSNR, it is noted that maximum PSNR value of 12.66dB is offered by the EFHE model whereas lower PSNR values of 10.44dB and 10.32dB has been offered by the EAE and ESE models under the Football dataset. On measuring the results interms of PSNR, it is noted that maximum PSNR value of 11.54dB is offered by the EFHE model whereas lower PSNR values of 0.9.46dB and 09.31dB has been offered by the EAE and ESE models under the Flowers dataset.

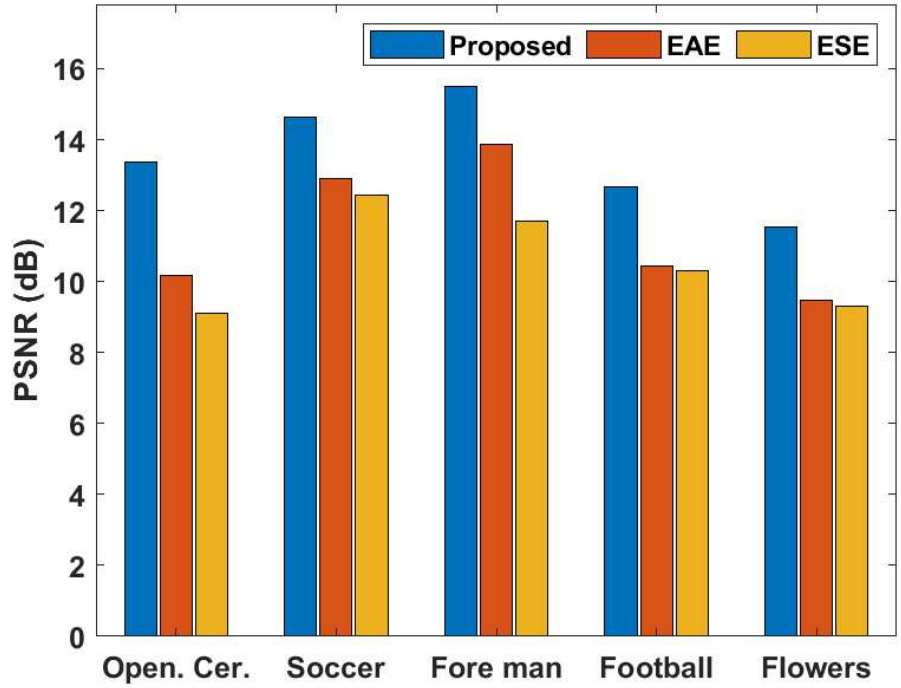


**Fig. 4.** PSNR analysis of various video encryption models

Fig. 5 examines the video encryption performance of the FEHE model interms of SSIM. When the results are investigated interms of SSIM, it is observed that highest PSNE value of 0.298 is obtained by the EFHE model whereas lower SSIM values of 0.265 and 0.216 has been offered by the EAE and ESE models under the opening ceremony dataset. When the results are investigated interms of SSIM, it is observed that highest PSNE value of 0.467 is obtained by the EFHE model whereas lower SSIM values of 0.410 and 0.316 has been offered by the EAE and ESE models under the Soccer dataset.

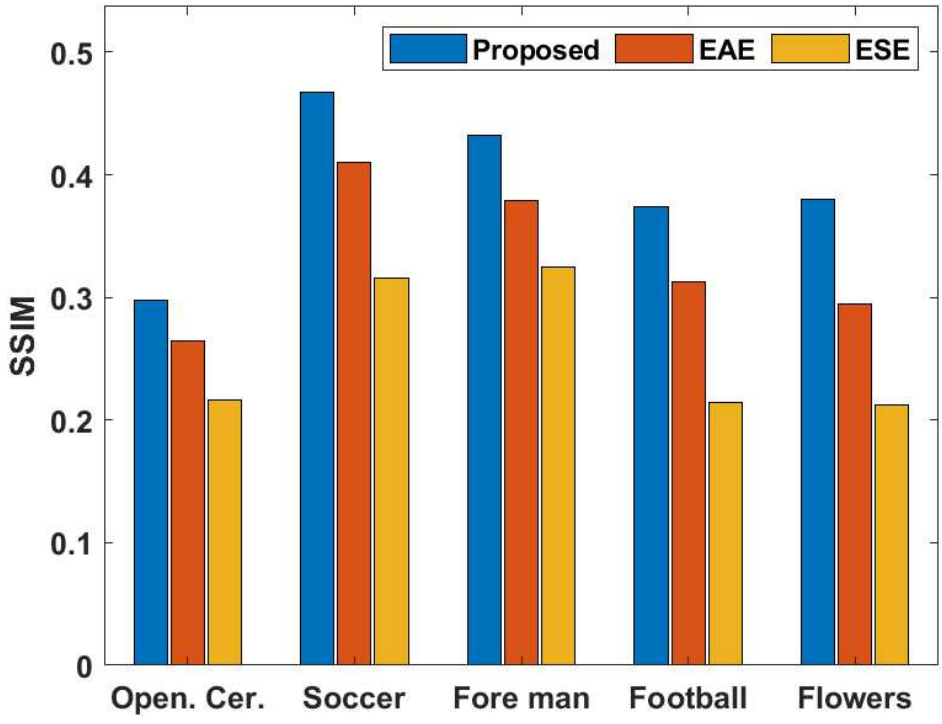


**Fig. 5.** SSIM analysis of various video encryption models

When the results are investigated interms of SSIM, it is observed that highest PSNE value of 0.432 is obtained by the EFHE model whereas lower SSIM values of 0.379 and 0.325 has been offered by the EAE and ESE models under the Fore man dataset. When the results are investigated interms of SSIM, it is observed that highest PSNE value of 0.374 is obtained by the EFHE model whereas lower SSIM values of 0.313 and 0.214 has been offered by the EAE and ESE models under the Football dataset. When the results are investigated interms of SSIM, it is observed that highest PSNE value of 0.380 is obtained by the EFHE model whereas lower SSIM values of 0.295 and 0.212 has been offered by the EAE and ESE models under the Flowers dataset.

### 4.2. Computation Complexity analysis

Table 2 examines the performance of the EFHE model interms of encryption and decryption time. Fig. 6 examines the video encryption performance of the FEHE model interms of encryption time. On measuring the results interms of encryption time, it is noted that least encryption time of 487.66s is required by the EFHE model whereas the EAR and ESE models requires a maximum encryption time of 500.22s and 508.12s respectively under the opening ceremony dataset.

**Table 2** Performance analysis of proposed with state of art methods in terms of Computational Complexity

| Videos | Encryption (s) | | | Decryption (s) | | |
|---|---|---|---|---|---|---|
| | **Proposed** | **EAE** | **ESE** | **Proposed** | **EAE** | **ESE** |
| **Opening Ceremony** | 487.66 | 500.22 | 508.12 | 1.38 | 1.47 | 1.50 |
| **Soccer** | 610.72 | 626.76 | 638.43 | 1.44 | 1.52 | 1.54 |
| **Fore man** | 165.84 | 177.98 | 179.94 | 0.49 | 0.57 | 0.58 |
| **Football** | 129.63 | 133.64 | 135.66 | 0.42 | 0.45 | 0.45 |
| **Flowers** | 185.94 | 190.87 | 194.09 | 0.59 | 0.66 | 0.67 |

On measuring the results interms of encryption time, it is noted that least encryption time of 610.72s is required by the EFHE model whereas the EAR and ESE models requires a maximum encryption time of 626.76s and 638.43s respectively under the Soccer dataset. On measuring the results interms of encryption time, it is noted that least encryption time of 165.84s is required by the EFHE model whereas the EAR and ESE models requires a maximum encryption time of 177.98s and 179.94s respectively under the Fore man dataset. On measuring the results interms of encryption time, it is noted that least encryption time of 129.63s is required by the EFHE model whereas the EAR and ESE models requires a maximum encryption time of 133.64s and 135.66s respectively under the Football dataset. On measuring the results interms of encryption time, it is noted that least encryption time of 185.94s is required by the EFHE model whereas the EAR and ESE models requires a maximum encryption time of 190.87s and 194.09s respectively under the Flowers dataset.

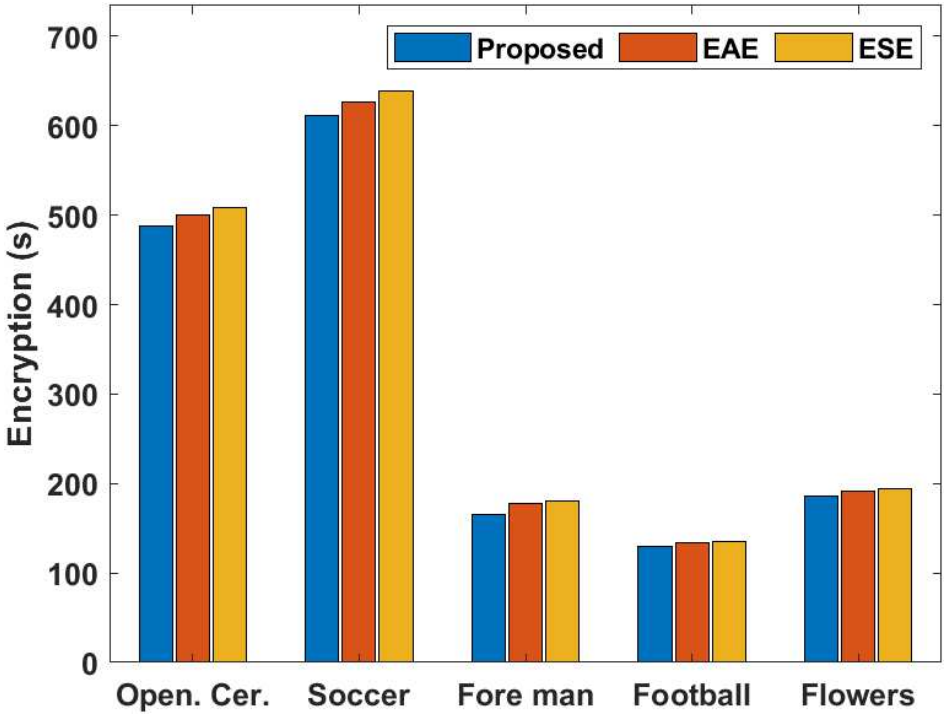


**Fig. 6.** Encryption time analysis of various video encryption models

Fig. 7 examines the video encryption performance of the FEHE model interms of Decryption time. On measuring the results interms of decryption time, it is noted that least encryption time of 1.38s is required by the EFHE model whereas the EAR and ESE models requires a maximum decryption time of 1.47s and 1.50s respectively under the opening ceremony dataset. On measuring the results interms of decryption time, it is noted that least encryption time of 1.44s is required by the EFHE model whereas the EAR and ESE models requires a maximum decryption time of 1.52s and 1.54s respectively under the Soccer dataset.

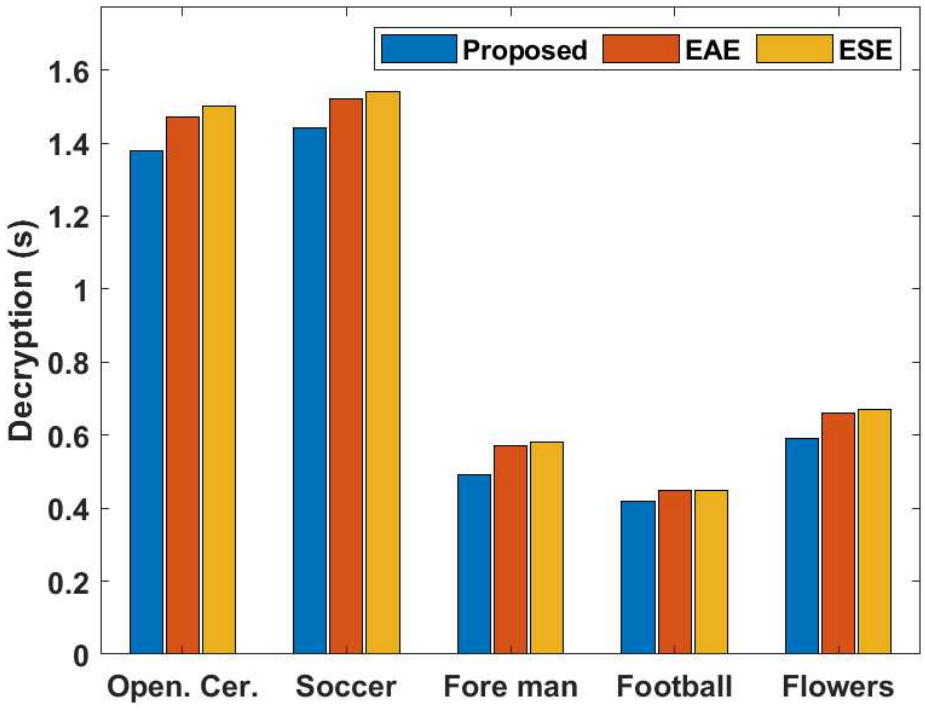


**Fig. 7.** Decryption time analysis of various video encryption models

On measuring the results interms of decryption time, it is noted that least encryption time of 0.49s is required by the EFHE model whereas the EAR and ESE models requires a maximum decryption time of 0.57s and 0.58s respectively under the Fore man dataset. On measuring the results interms of decryption time, it is noted that least encryption time of 0.4s is required by the EFHE model whereas the EAR and ESE models requires a maximum decryption time of 0.4s and 0.45s respectively under the Football dataset. On measuring the results interms of decryption time, it is noted that least encryption time of 0.59s is required by the EFHE model whereas the EAR and ESE models requires a maximum decryption time of 0.66s and 0.67s respectively under the Flowers dataset.

### 4.3. Bit rate analysis

Table 3 and Fig. 8 provide a detailed explanation of the FEHE model with compared methods interms of bit rate. On measuring the results interms of bit rate, it is defined that the EFHE and EAE models attains a minimum bit rate of 0.07 whereas slightly higher bit rate is offered by EAE and ESE with the bit rates of 0.07 and 0.09 under the applied opening ceremony dataset. On measuring the results interms of bit rate, it is defined that the EFHE and EAE models attains a minimum bit rate of 0.13 whereas slightly higher bit rate is offered by EAE and ESE with the bit rates of 0.15 and 0.18 under the applied Soccer dataset. On measuring the results interms of bit rate, it is defined that the EFHE and EAE models attains a minimum bit rate of 0.08 whereas slightly higher bit rate is offered by EAE and ESE with the bit rates of 0.10 and 0.13 under the applied Fore man dataset. On measuring the results interms of bit rate, it is defined that the EFHE and EAE models attains a minimum bit rate of 0.11 whereas slightly higher bit rate is offered by EAE and ESE with the bit rates of 0.13 and 0.15 under the applied Football dataset.

**Table 3** Performance analysis of EFHE with state of art methods in terms of Bit rate

| **Videos** | **Bitrates (%)** | | |
|---|---|---|---|
| | **EFHE (%)** | **EAE (%)** | **ESE (%)** |
| Opening Ceremony | 0.07 | 0.07 | 0.09 |
| Soccer | 0.13 | 0.15 | 0.18 |
| Fore man | 0.08 | 0.10 | 0.13 |
| Football | 0.11 | 0.13 | 0.15 |
| Flowers | 0.10 | 0.14 | 0.15 |

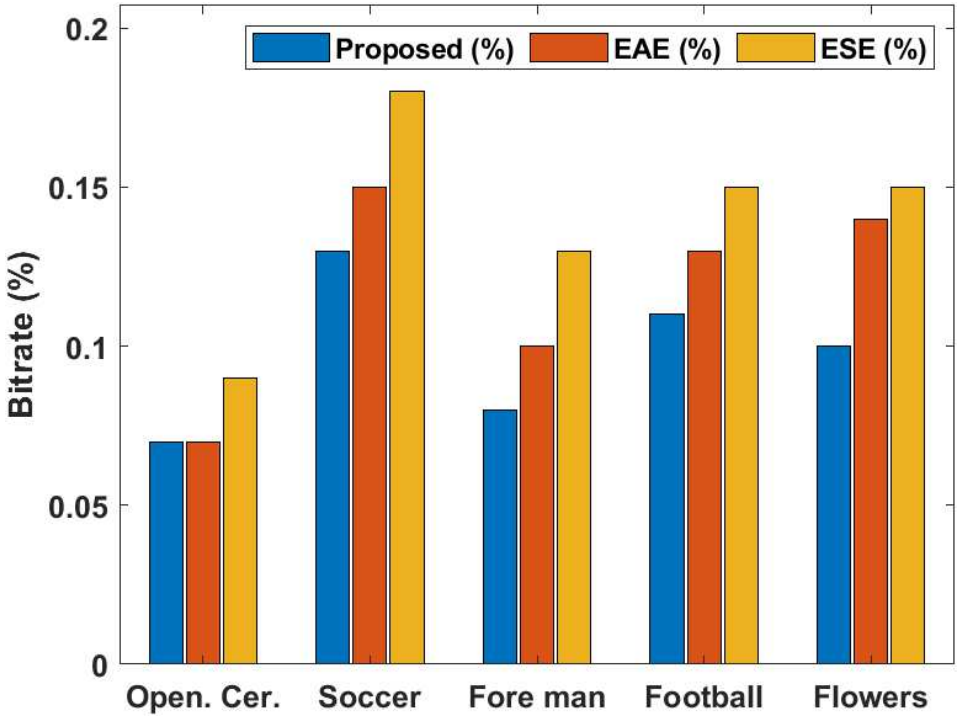


**Fig. 8.** Bit rate analysis of various video encryption models

On measuring the results interms of bit rate, it is defined that the EFHE and EAE models attains a minimum bit rate of 0.10 whereas slightly higher bit rate is offered by EAE and ESE with the bit rates of 0.14 and 0.15 under the applied Flowers dataset.

### 4.4. Brute Force attack analysis

Table 4 examines the results attained by different methods interms of PSNR under brute force attack. Under the encryption of frame 1, the EFHE model attains higher PSNR value of 13.6dB whereas slightly lower PSNR values of 12.2dB and 11.8dB has been attained by the EAE and ESE models. Similarly, under the encryption of frame 2, the EFHE model attains higher PSNR value of 13.4dB whereas slightly lower PSNR values of 12.1dB and 11.6dB has been attained by the EAE and ESE models. Likewise, under the encryption of frame 3, the EFHE model attains higher PSNR value of 13.1dB whereas slightly lower PSNR values of 13.2dB and 11.9dB has been attained by the EAE and ESE models. In the same time, under the encryption of frame 4, the EFHE model attains higher PSNR value of 12.4dB whereas slightly lower PSNR values of 11.4dB and 10.6dB has been attained by the EAE and ESE models. Simultaneously, under the encryption of frame 5, the EFHE model attains higher PSNR value of 13.9dB whereas slightly lower PSNR values of 13.6dB and 12.4dB has been attained by the EAE and ESE models. In addition, under the encryption of frame 6, the EFHE model attains higher PSNR value of 11.4dB whereas slightly lower PSNR values of 10.2dB and 09.8dB has been attained by the EAE and ESE models. Besides, under the encryption of frame 7, the EFHE model attains higher PSNR value of 11.8dB whereas slightly lower PSNR values of 10.4dB and 10.2dB has been attained by the EAE and ESE models.

**Table 4** Analysis of Brute Force Attack

| Frame Number | PSNR (dB)) | | |
|---|---|---|---|
| | **Proposed** | **EAE** | **ESE** |
| 1 | 13.6 | 12.2 | 11.8 |
| 2 | 13.4 | 12.1 | 11.6 |
| 3 | 13.1 | 13.2 | 11.9 |
| 4 | 12.4 | 11.4 | 10.6 |
| 5 | 13.9 | 13.6 | 12.4 |
| 6 | 11.4 | 10.2 | 09.8 |
| 7 | 11.8 | 10.4 | 10.2 |
| 8 | 11.9 | 10.8 | 09.6 |
| 9 | 12.6 | 11.2 | 10.4 |
| 10 | 12.9 | 12.3 | 11.8 |

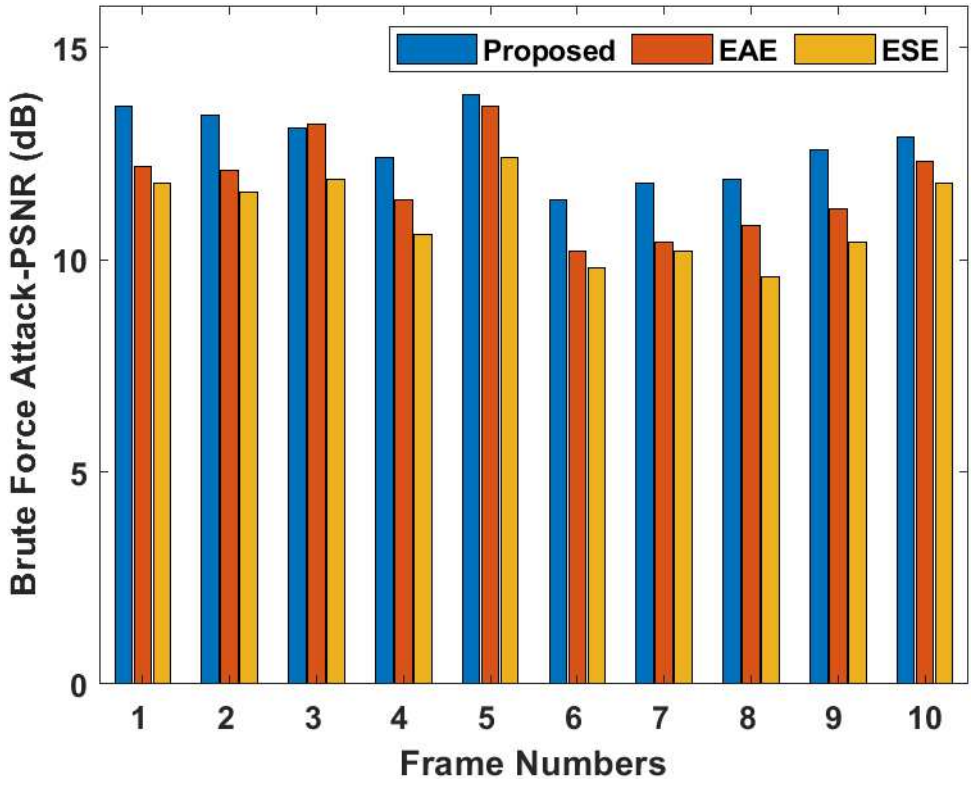


**Fig. 9.** Analysis of Brute force attack for diverse video encryption models

Moreover, under the encryption of frame 8, the EFHE model attains higher PSNR value of 11.9dB whereas slightly lower PSNR values of 10.8dB and 09.6dB has been attained by the EAE and ESE models. Furthermore, under the encryption of frame 9, the EFHE model attains higher PSNR value of 12.6dB whereas slightly lower PSNR values of 11.2dB and 10.4dB has been attained by the EAE and ESE models. At last, under the encryption of frame 10, the EFHE model attains higher PSNR value of 12.9dB whereas slightly lower PSNR

values of 12.3dB and 11.8dB has been attained by the EAE and ESE models. These values ensured that the presented EFHE model offers better security over the compared methods in a considerable way.

## 5. Conclusion

This paper has introduced an effective video encryption technique named as EFHE model by the incorporation of enhanced FHE with multiplication and addition operations along with a novel key generation scheme. The presented model has been validated by the use of a set of five benchmark videos namely Opening Ceremony, Soccer, Foreman, Football and Flowers. The results are validated in terms of PSNR, SSIM, computation complexity, bit rate, and brute force attack analysis. The experimental outcome pointed out the superior performance of the presented EFHE model over the compared methods in a significant way. In future, the video compression then encryption scheme can be introduced to effectively compress the video and then encrypts it to avail the benefits of both compression and encryption process.

**Acknowledgement**

This research work has been financially supported by RUSA Phase-2.0/Ph.D Fellowship/2019, Alagappa University, Karaikudi, Tamilnadu, India.

**Declarations**

The authors declares that there is no conflict of interest.

## References

[1] W. Quan, Y. Liu, H. Zhang, and S. Yu, “Enhancing crowd collaborations for sofware defned vehicular networks,” IEEE Communications Magazine, vol. 55, no. 8, pp. 80–86, 2017.

[2] B. Feng, H. Zhang, H. Zhou, and S. Yu, “Locator/Identifer Split Networking: A Promising Future Internet Architecture,” IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2927– 2948, 2017.

[3] H. Zhang, W. Quan, H.-C. Chao, and C. Qiao, “Smart identifer network: A collaborative architecture for the future internet,” IEEE Network, vol. 30, no. 3, pp. 46–51, 2016.

[4] C. Yuan, Z. Xia, and X. Sun, “Coverless image steganography based on SIFT and BOF,” Journal of Internet Technology, vol. 18, no. 2, pp. 209–216, 2017.

[5] F. Song, Z. Ai, J. Li et al., “Smart Collaborative Caching for Information-Centric IoT in Fog Computing,” Sensors, vol. 17, no. 11, p. 2512, 2017.

[6] Q. Wu, M. Zhang, R. Zheng, Y. Lou, and W. Wei, “A QoSSatisfed Prediction Model for Cloud-Service Composition Based on a Hidden Markov Model,” Mathematical Problems in Engineering, vol. 2013, Article ID 387083, 7 pages, 2013.

[7] J. Li, W. Yao, Y. Zhang, H. L. Qian, and J. G. Han, “Flexible and fne-grained attribute-based data storage in cloud computing,” IEEE Transactions on Services Computing, vol. 10, no. 5, pp. 785– 796, 2017

[8] Q. Wu, X. Zhang, M. Zhang, Y. Lou, R. Zheng, and W. Wei, “Reputation Revision Method for Selecting Cloud Services Based on Prior Knowledge and a Market Mechanism,” Te Scientifc World Journal, vol. 2014, Article ID 617087, 9 pages, 2014.

[9] Z. Fu, K. Ren, and J. Shu, “Enabling personalized search over encrypted outsourced data with efficiency improvement,” IEEE Transactions on Parallel Distributed Systems, vol. 27, no. 9, pp. 2546–2559, 2016.

[10] Z. Brakerski and V. Vaikuntanathan, “Efcient fully homomorphic encryption from (standard) LWE,” in Proceedings of the IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS ’11), pp. 97–106, Palm Springs, Calif, USA, October 2011.

[11] R. Zheng, J. Chen, M. Zhang, Q. Wu, J. Zhu, and H. Wang, “A collaborative analysis method of user abnormal behavior based on reputation voting in cloud environment,” Future Generation Computer Systems, vol. 83, pp. 60–74, 2018.

[12] M. Zhang, M. Yang, Q. Wu, R. Zheng, and J. Zhu, “Smart perception and autonomic optimization: A novel bio-inspired hybrid routing protocol for MANETs,” Future Generation Computer Systems, vol. 81, pp. 505–513, 2018.

[13] M. Zhang, C. Xu, J. Guan, R. Zheng, Q. Wu, and H. Zhang, “A Novel Physarum-Inspired Routing Protocol for Wireless Sensor Networks,” International Journal of Distributed Sensor Networks, vol. 2013, Article ID 483581, 12 pages, 2013

[14] R. L. Rivest, L. Adleman, and M. L. Dertouzos, On Data Banks And Privacy Homomorphism Proc of Foundations of Secure Computation, Academic Press, New York, NY, USA, 1978.

[15] M. Liu and W. An, “Fully Homomorphic Encryption and Its Application,” Journal of Computer Research & Development, vol. 51, no. 12, pp. 2593–2603, 2014.

[16] H. Yan, G. Chen, and T. Han, “Scope of application of homomorphic encryption algorithm and improvement of efciency and application,” Computer Engineering and Design, vol. 38, no. 2, pp. 318–322, 2017.

[17] H. Demin and Y. Xing, “Dynamic cloud storage data integrity verifying method based on homomorphic tags,” Application Research of Computers, vol. no. 5, pp. 1362–1365, May 2014

[18] Y. Zhu, H. Wang, Z. HU et al., Cooperative Provable Data Possession, Peking University and Arizona University, Beijing, China, 2010.

[19] X. Cao, C. Moore, M. O’Neill, E. O’Sullivan, and N. Hanley, “Optimised multiplication architectures for accelerating fully homomorphic encryption,” Institute of Electrical and Electronics Engineers. Transactions on Computers, vol. 65, no. 9, pp. 2794– 2806, 2016.

[20] J. Chen, H. Ma, and D. Zhao, “Private data aggregation with integrity assurance and fault tolerance for mobile crowdsensing,” Wireless Networks, vol. 23, no. 1, pp. 131–144, 2017.

[21] S. Wang, J. Zhou, and J. Liu, “An Efcient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing,” IEEE Transactions on Information Forensics Security, vol. 11, no. 6, pp. 1265–1277, 2016.

[22] A. Li, S. Tan, and Y. Jia, “A method for achieving provable data integrity in cloud computing,” Te Journal of Supercomputing, pp. 1–17, 2016

[23] C. Gentry, A. Sahai, and B. Waters, "Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based," Proceedings of CRYPTO 2013, vol. 8042, no. 1, pp. 75–92, 2013.

[24] Jan, M.A., Zhang, W., Usman, M., Tan, Z., Khan, F. and Luo, E., 2019. SmartEdge: An end-to-end encryption framework for an edge-enabled smart city application. *Journal of Network and Computer Applications*, *137*, pp.1-10.

[25] T. Wu, H. Wang, and Y. P. Liu, "Optimizations of Brakerski's fully homomorphic encryption scheme," in Proceedings of the 2nd International Conference on Computer Science and Network Technology, ICCSNT 2012, pp. 2000–2005, December 2012.

[26] Cheng, S., Wang, L., Ao, N. and Han, Q., 2020. A Selective Video Encryption Scheme Based on Coding Characteristics. Symmetry, 12(3), p.332.

[27] Wang, X., Luo, T. and Li, J., 2018. A More Efficient Fully Homomorphic Encryption Scheme Based on GSW and DM Schemes. *Security and Communication Networks*, *2018*.

[28] Chao, F.E.N.G. and Yang, X.I.N., 2014. Fast key generation for Gentry-style homomorphic encryption. *The Journal of China Universities of Posts and Telecommunications*, *21*(6), pp.37-44.

[29] Thiyagarajan, K., Lu, R., El-Sankary, K. and Zhu, H., 2018. Energy-Aware Encryption for Securing Video Transmission in Internet of Multimedia Things. *IEEE Transactions on Circuits and Systems for Video Technology*, *29*(3), pp.610-624.

[30] B. Boyadjis, C. Bergeron, B. Pesquet-Popescu, and F. Dufaux, "Extended selective encryption of h.264/avc (cabac)- and hevc-encoded video streams," IEEE Transactions on Circuits and Systems for Video Technology, vol. 27, no. 4, pp. 892–906, April 2017.

**N.Geetha** is a Ph.D Scholar in the Department of Computer Applications, Alagappa University, Karaikudi. Tamilnadu, India.Her area of interest includes Video Processing (Encryption) and Cloud Security.

**K.Mahesh** is a Professor in Department of Computer Applications, Alagappa University, Karaikudi, India. He has Published many papers in Peer-Reviewed and Reputed Journal and has 25 years of experience in teaching. His research interests are Video Segmentation, Video Processing and Image Processing.