electronics

MDPI

Article

Digital Image Identification and Verification Using Maximum and Preliminary Score Approach with Watermarking for Security and Validation Enhancement

Shrikant Upadhyay [1], Mohit Kumar [2], Aditi Upadhyay [3], Sahil Verma [4], Kavita [4], A. S. M. Sanwar Hosen [5,*], In-Ho Ra [6,*], Maninder Kaur [7] and Satnam Singh [8]

1 Department of Electronics & Communication Engineering, Cambridge Institute of Technology, Tatisilwai, Ranchi 835103, Jharkhand, India
2 Department of IT, MIT Art, Design and Technology University, Pune 412201, Maharashtra, India
3 School of Engineering, Department of ECE, Jaipur National University, Jaipur 91141, Rajasthan, India
4 Department of CSE, Uttaranchal University, Dehradun 248007, Uttarakhand, India
5 Department of Artificial Intelligence and Big Data, Woosong University, Daejeon 34606, Republic of Korea
6 School of Computer, Information and Communication Engineering, Kunsan National University, Gunsan 54150, Republic of Korea
7 Department of Computer Science and Applications, Guru Gobind Singh College for Women, Chandigarh 160019, Punjab, India
8 Department of CSE, SGT University, Gurugram 122505, Haryana, India
* Correspondence: sanwar@wsu.ac.kr (A.S.M.S.H.); ihra@kunsan.ac.kr (I.-H.R.)

Abstract: Digital face approaches possess currently received awesome attention because of their huge wide variety of digital audio, and visual programs. Digitized snapshots are progressively more communicated using an un-relaxed medium together with cyberspace. Consequently, defence, clinical, medical, and exceptional supervised photographs are essentially blanketed towards trying to employ it; such controls ought to damage such choices constructed totally based on those pictures. So, to shield the originality of digital audio/visual snapshots, several approaches proposed. Such techniques incorporate traditional encoding, breakable and nominal breakable watermarking with virtual impressions which are based upon the material of image content. Over the last few decades, various holistic approaches are proposed for improving image identification and verification. In this paper, a combination of both the feature level and score level of different techniques were used. Image is one of the identities of a person which reflects its emotions, feeling, age etc. which also helps to gather an information about a person without knowing their name, caste, and age and this could be not of much importance when it is used for domestic or framing applications. To secure the originality of digital audio/visual impressions many methods come into pictures and are proposed which include digital signatures, watermarking, cryptography, and fragile depend upon face contents. The objective of this research article is to identify & verify real-time video images using feature and score levels using watermarking that will help to judge the authenticity of any images at the initial stage by extracting the features which are evaluated by following an algorithm known as Viterbi and where input data is changed initially into an embedded treat or state then the matrix is evaluated of achieved transformation and on this basis preliminary score estimation will be generated after many iterations for each image that will help in validation. Finally, the tested image will be verified using several approaches to protect and provide security to the original image being verified. This approach may be useful for different surveillance applications for real-time image identification and verification. Also, measurement of accuracy was done by reconfiguring the HMM to identify the constant segmentation and feature removal of the image was settled by initializing parameters and teaching the image feature using the algorithm "Viterbi".

Keywords: watermarking; authentication; security; HMM; Viterbi algorithm; score level

Citation: Upadhyay, S.; Kumar, M.; Upadhyay, A.; Verma, S.; Kavita; Hosen, A.S.M.S.; Ra, I.-H.; Kaur, M.; Singh, S. Digital Image Identification and Verification Using Maximum and Preliminary Score Approach with Watermarking for Security and Validation Enhancement. *Electronics* **2023**, *12*, 1609. https://doi.org/10.3390/electronics12071609

Received: 17 February 2023
Revised: 15 March 2023
Accepted: 20 March 2023
Published: 29 March 2023

1. Introduction

In the past few years face identification and its verification received great attention in computer vision, pattern recognition and biometric communities. Common attraction among researchers motivated by the phenomenal capability to identify a human faces with evidence such that people's occupations are related both in multimedia and daily routine. The facial analysis involves extracting or gathering information like age, gender, pose, landmark, naming etc. It includes different applications as well as law imposition, face biometrics for transactions, self-driving vehicles, active verification on devices etc. Validation and recognition of face systems basically consist of basic three steps. Starting, the stage consists of an identifier for confining profile in faces is required and belongings of profiles identifier are strong to variations in illuminations, scale and pose. Also, an efficient face identifier should be able to handle output constantly with a well confining limited area. The second stage localizes the facial indicators like the tip of the nose, view base, point of ear lobes, jaw corner etc. Such indicators are then worn to arrange profiles (faces) with ease consequence of scaling and in-level spinning. The last and third stage is of attribute separator which encrypts the naming statistics in a high-dimension locator. Such complete descriptions are worn to evaluate a similar point or outcome in the middle of similar profiles. A fruitful attribute separator capable to handle delusions found by back stages in the queue: profile alignment, face recognition and indicator finding [1]. The method that we follow to do a measurement of accuracy is by first reconfiguring Hidden Markov to take out the steady subdivision the separation of attributes for images using parameter reconfiguration and teach the characteristics of the image following an algorithm known as Viterbi. Additionally, an image at input now transforms into an embedded and super state and the matrix obtained from the transformation is calculated using a higher outcome estimation of each set of the face. Now, we verify the higher outcome parameters for the Markov model and check the condition if it detects 'Yes' or if it will go for some other new attribute separator to detect the 'No' condition [2,3]. The steps involved in image identification and its verification are shown in Figure 1.

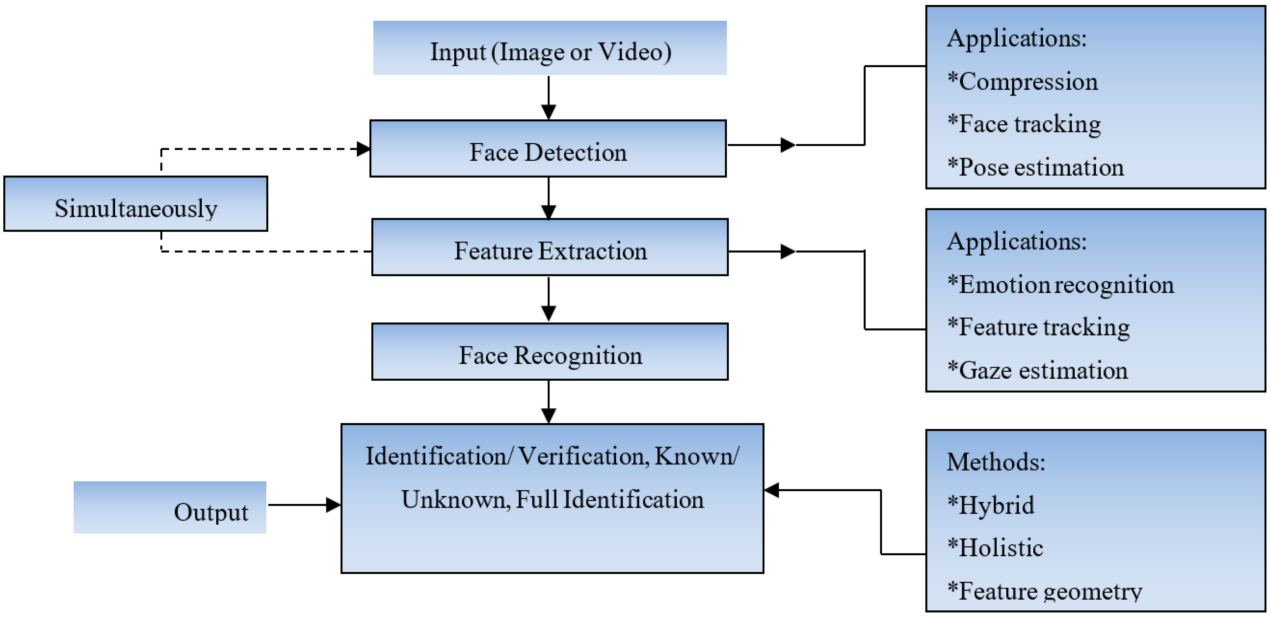

Figure 1. Steps involved in identification and verification.

The profile (face) has many benefits that force it to be one of the efficient bioscrypt distinguishing qualities. First, the profile face reflects internal emotions (affections) of happiness or sadness (concern) including the person's approximate age and identity. Second, even at a long distance, the face biometric is easy to capture. And this feature makes

face identification crucial in person recognition as well as in human-computer interaction. The profile face bioscrypt is impressed by a variety of extrinsic and natural variations like lighting, pose, age and expressions. In the past, an outstanding refinement was observed in the staging of the profile face identification, but quiet under the tolerable levels found in various applications. A modern attempt has mainly concentrated on different features, 3D (3-dimensional) prototypes and pictorial inputs to control the execution of additional demand in 2-dimensional profile still image identification [4]. Face geometrically is a 3D space sum of a large number of polygons that can be represented by facial features and pixels related to the face geometry. Image data computationally can be represented in vector form. For example, $x \times y$ with 2-dimensional image be depicting using vector $P\ \varepsilon\ R^{xy}$, and sequencing components of pixels by a succession of every column & row of images. Different face with different emotions is shown in Figure 2.

Figure 2. Human faces with emotions.

Where, $P = (P_1,\ P_2 \ldots\ P_i \ldots\ P_N)$, denotes the $n \times N$ fact matrix, where P_i is a profile direction of dimension n, progression from $x \times y$ profile image, where $n = x \times y$ indicates the aggregate number of pixel.

The proposed model in terms of novelty deals with the fact that the identity of the face in background is fixed and known which is normally not present in earlier existing models. It also identifies the face succession from the given input and tracks the identified face over the successive frame that maintains the dimensional construction of data without any supports of blocks.

2. Related Work

Walton in the year 1995 [5] proposed the first approach based on watermarking where image verification was done by fragile watermarking where only image facts are used to develop the watermark. This approach used the placing technique using checksum and least significant bit with a grey quantity of the most significant seven selected pseudo-randomly captured pixels. This approach localizes and detects but not having a repairing facility. In the year 2020 [6] proposed an algorithm that gain more attention where a large number of '*N*' is used for evaluating the checksums and this size directly affects the detecting probability manipulations. H. Cheng in the year 2019 [7] proposed a method based on a secret key used to create a binary function and this function maps integers from interval {0, 1, 2, ...255} per colour image which is further used as code to calculate the grey level. M.T. Bhatti & W. Fang [8,9] in the year 20,211 proposed a method to prevent attack from vector quantification to prevent attack from vector quantification based on a private public key systems and minimize the quantification attack.

Lee [10] in the year 2021 proposed a method to validate colour images using fragile watermarking where colour images are decomposed into three different parts for their protection also this colour component is used to hide the facts of images. Byun SC and K. Seth [11,12] in the year 2002 & 2021 proposed a technique that converts the grey level of original version of image in interval $(-127, 128)$ and break image into 8×8 blocks and separate each blocks using cosine discrete transform. In [13] authors discussed digital watermarking approach to provide authentication and ownership for audio, videos and images where watermarking is first transformed and in way to encrypt the sequence of randomly generated pixels for key selection.

In [14] authors discussed a watermarking approach in which dropped a mark in program and protecting its functionality and no one has right to uncover the mark without affecting the functionality. In [15] authors proposed a technology of watermarking for industries to provide security to their leased or hired data. In this paper Fractal and Spatial algorithm watermarking was considered to improve the protection of data compression. In Spatial approach there is no need for transforming the computation of embedding watermarking. Here nine co-ordinates minimum considered for its implementation.

In [16] authors proposed a method for multimedia facts copyright protection using digital watermarking as it helps to reduce the increasing overhead. Text or numbers, videos, and images are considered for the analysis where information is not embedded in the frame throughout the data. Cryptography which is based on an unseeing image watermarking approach was presented to increase security. Scrambling watermarks with different attacks like Gaussian noise, median filtering, rotation etc. was also discussed in many papers.

The existing approaches face the problems of protecting their functionality in protecting compressed data. It also arises the issue of copyright protection which increases the overhead. The decomposition of images increases the chances of validation and verification. The proposed model takes care of such issues in the training and testing phase process. This process increases the authentication and validation to become more secure without affecting the original version of images.

3. Maximum and Preliminary Score Approach

Face identification at the preliminary will be done using Hidden Markov model (HMM) with unobserved states which does not reflect its identity directly which generate token in form of sequence that are generated to highlight the information of sequence state [17,18]. Variable $a(t) = \{a_1, a_2, a_3\}$ is the state (hidden) with time't' and variable $b(t) = \{b_1, b_2, b_3\}$ at time't'. Now, using gray scale for 1-D HMM the facial area covers hairs, forehead, eyes, nose & mouth follow in up-to-down in order. The face recognition system is shown in Figure 3.

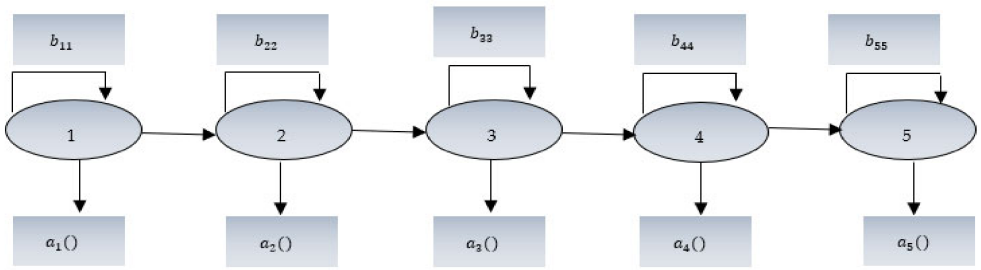

Figure 3. Face recognition using HMM (from left-to-right).

It is observed here that each facial area is devoted to a state from left to right 1-D but, the embedded Hidden Markov in 2-D have been used for image representation and recognition, $Y = \{Y_t\} = \{Y_{tpq}\}$ using spatial indices (p, q) and designed by HMM arrangement which consist of a set called super state S_{pq} which does not allow any type of crossing between embedded state and super state. A total super state contains five characterizations which cover the brow, eyelet, hooter, jaw & chin in upright path properly with beginning condition and conditional probabilities. $\{\prod v, B_v\} = \left\{\pi_{fn}; b_{f_{nFn+1}}\right\}$. Now, every state (super) itself a 1-D standard Markov model hold implant state for facial designing characteristics and have 21 (twenty one) embedded states in horizontal direction [19,20].

$$b_{pqr}(x) = P(x\ I\ r_{pqr},\ P_b) = \sum_{l_{pq}}^{N_l} w_{pqr} l_{pq}\ N(x\ I\ \mu_{pqr} l_{pq}, \sum_{pqr} l_{pq}) \quad (1)$$

The distribution of two different videos to attain values of different score levels is shown in Figure 4a,b.

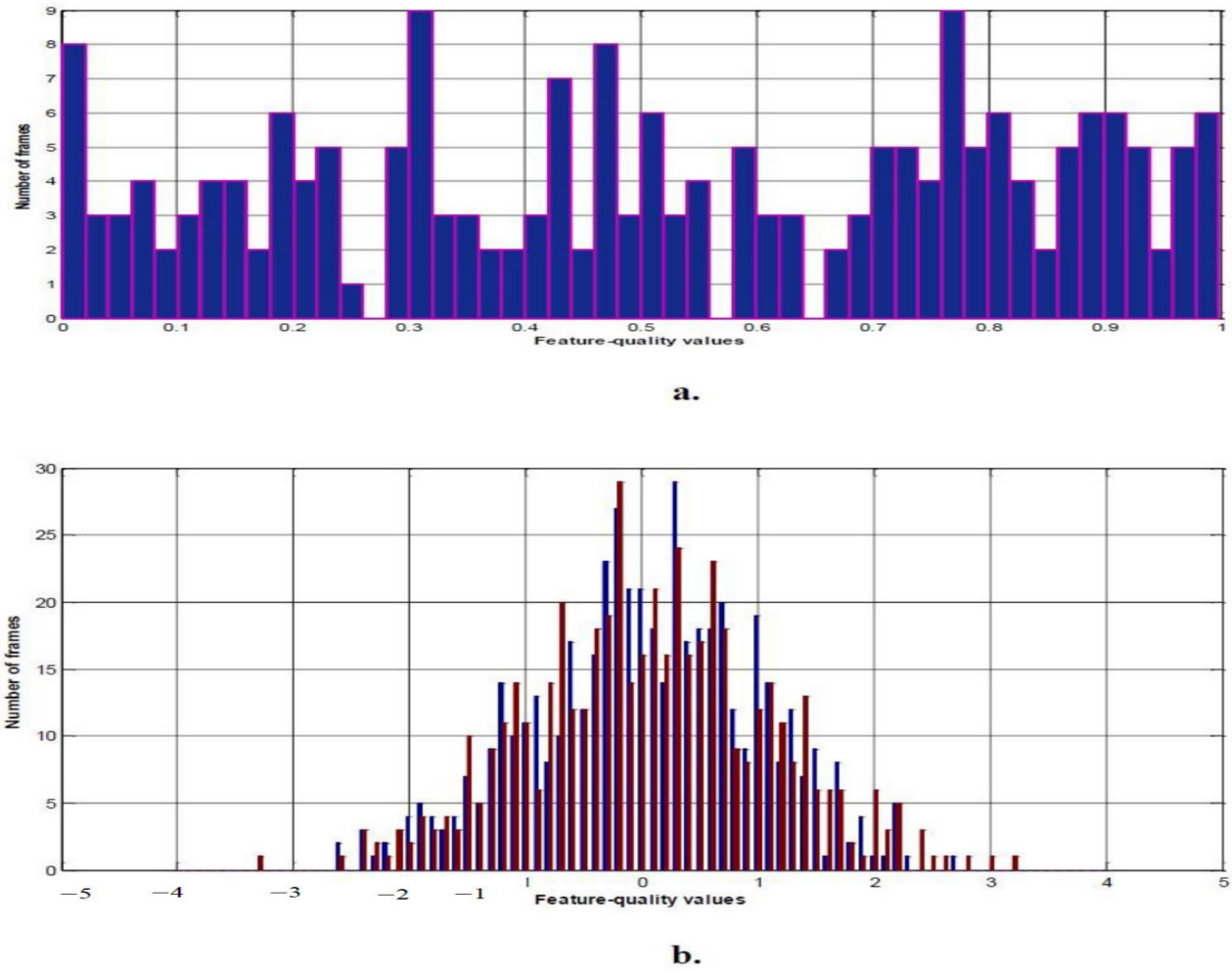

Figure 4. Feature distribution Feature distribution for two dissimilar videos (**a**,**b**) where some value reaches to zero where as some feature attain value close to one which means high fidelity frame have maximum score where as poor frames have minimum score. Here, $x-$axis represents feature quality values and $y-$axis represents number of frames.

4. Image Authentication

Authentication means verifying real value or content which is achieved without being tempered. As, in real-time applications, it is very difficult to maintain its original identity because of the number of reasons being generated by surrounding or by the communication devices. Image authentication does not accept any tempered image data. The conventional approach constructed on coding evaluates content evidence from portrayal utilizing a function called 'hash' [21,22]. This hash function is altered and coded using an exclusive key for the transmitter and then connected to the portrayal. So, for higher security data interchange between matters, the function hash can code taking support of the public key of the beneficiary [23]. The authentication and verification are depicted in Figure 5a,b.

The recipient evaluates the hash from received image and it was attached to the recovered images and decrypted with the help of private key. Hash evaluation of images using columns and line functions are obtained and it will be stored and correlate with the obtained value from every column and line of profile image to be verified [24,25]. Mismatch if any in hash function was observed the profile is proclaimed to be tempered else announced genuine. Since hash functions quite responsive to any slight changes in binary data or profile discrete components and this puts limits on image verification for many applications. Robust watermarking approach is used to create some form of watermark and put to profile to be sheltered hence that any changes found must show

in placed watermark. Confirming the existence of the placed watermark approves the reliability of image and finally generalized of damaged areas [26,27]. Such method doesn't accept any distorted image and authenticate only if all its pixels remain constant. The generation and its verification are depicted in Figure 6a,b.

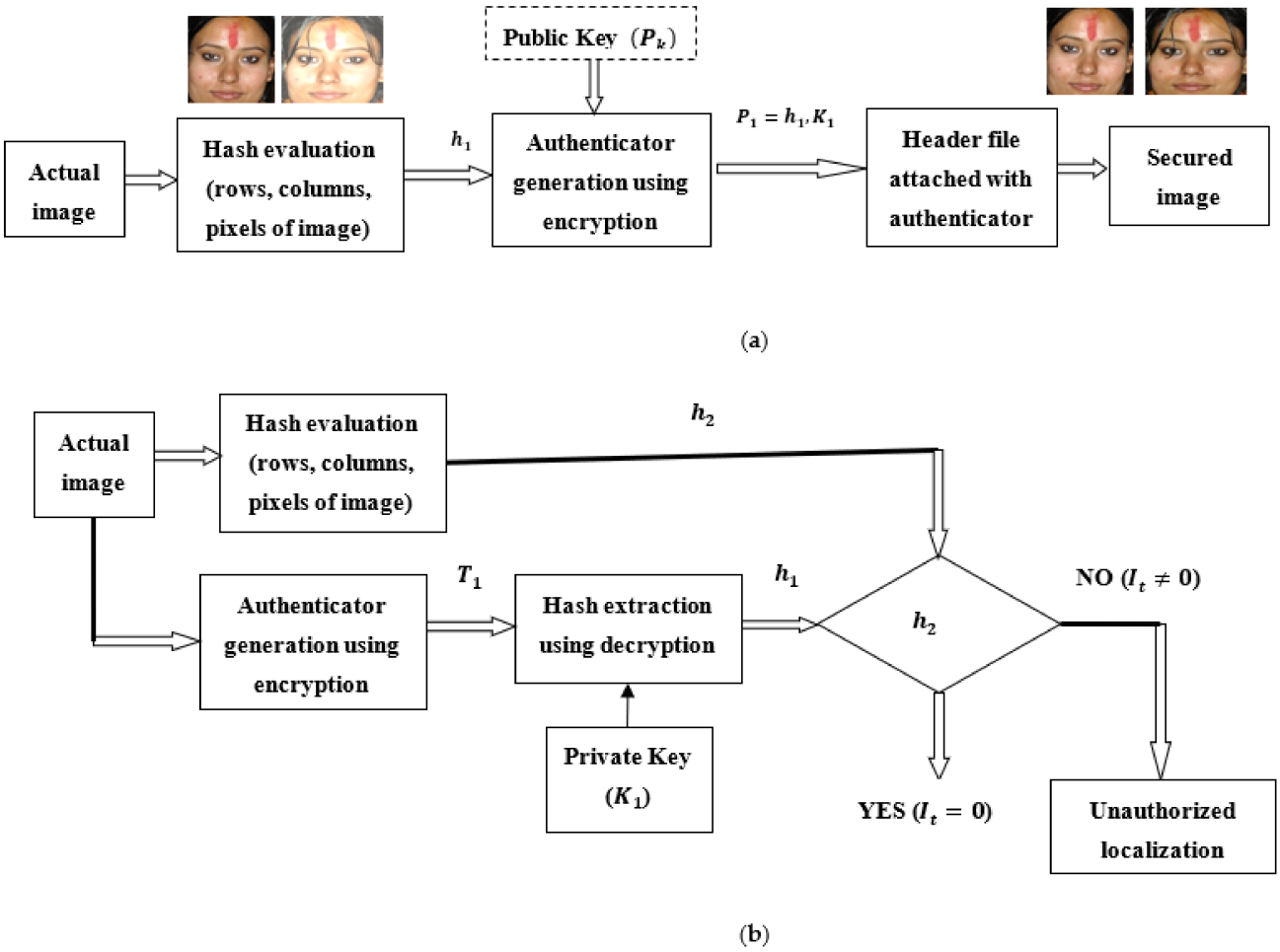

Figure 5. System for image authentication using cryptography following public & private key; (**a**) authenticator generator; (**b**) authenticity verification.

Frangible watermarking algorithms depend upon tidemark formation from profile identity and tidemark is evaluated using set of profile discrete components. The set of pixels taken from the secret key SK_1 evaluated tidemark may be decoded using a secret key SK_3 with minimum notable bit of some another carriage. To increase the security of algorithm carriage of discrete components may be identified by another confidential clue SK_2. Digital signature purpose is to sign a document in electronics for and used when any document is written, signing a contract or withdrawing money from a bank. So, digital authentication can be transferred digitally using registered letter [28]. Several issues are experienced with digital authentication. Initially, digital signature requires algorithm that has to be attached with the signature for electronics transfer. Second, second problem related with its verification and signature authentication. Example: When one's registration is verified by differentiating with its verified one while purchasing anything using credit/debit card. So, this authentication approach is not strong enough, as it will be quite easy to copy the authentication of certified person [29–31]. Therefore, digital verification will be tested by taking persons having knowledge of confirmation algorithm. Applying an electronics authentication algorithm put straight to the profile which may result in conditions where profile details have not been tempered, the algorithm denotes the profile as false. As a

result, changes to surviving programmed signatures methods should perform missing by illustrating the facts that required being indicated i.e., profile details must be indicated rather than profile features alone. Electronically hash value indicating using surviving programming signature like a public key or private key can increase the overall security. And verification procedure depends on the image signature which could be extracted from the attached signature and by comparing it with its original signature. Function using hash operates on the information of any duration to achieve stable proportion hash '*h*' known as information digest:

$$h = H(X) \tag{2}$$

where, $'H'$ indicates function of hash and proportion of $'h'$ is normally lower than $'X'$.

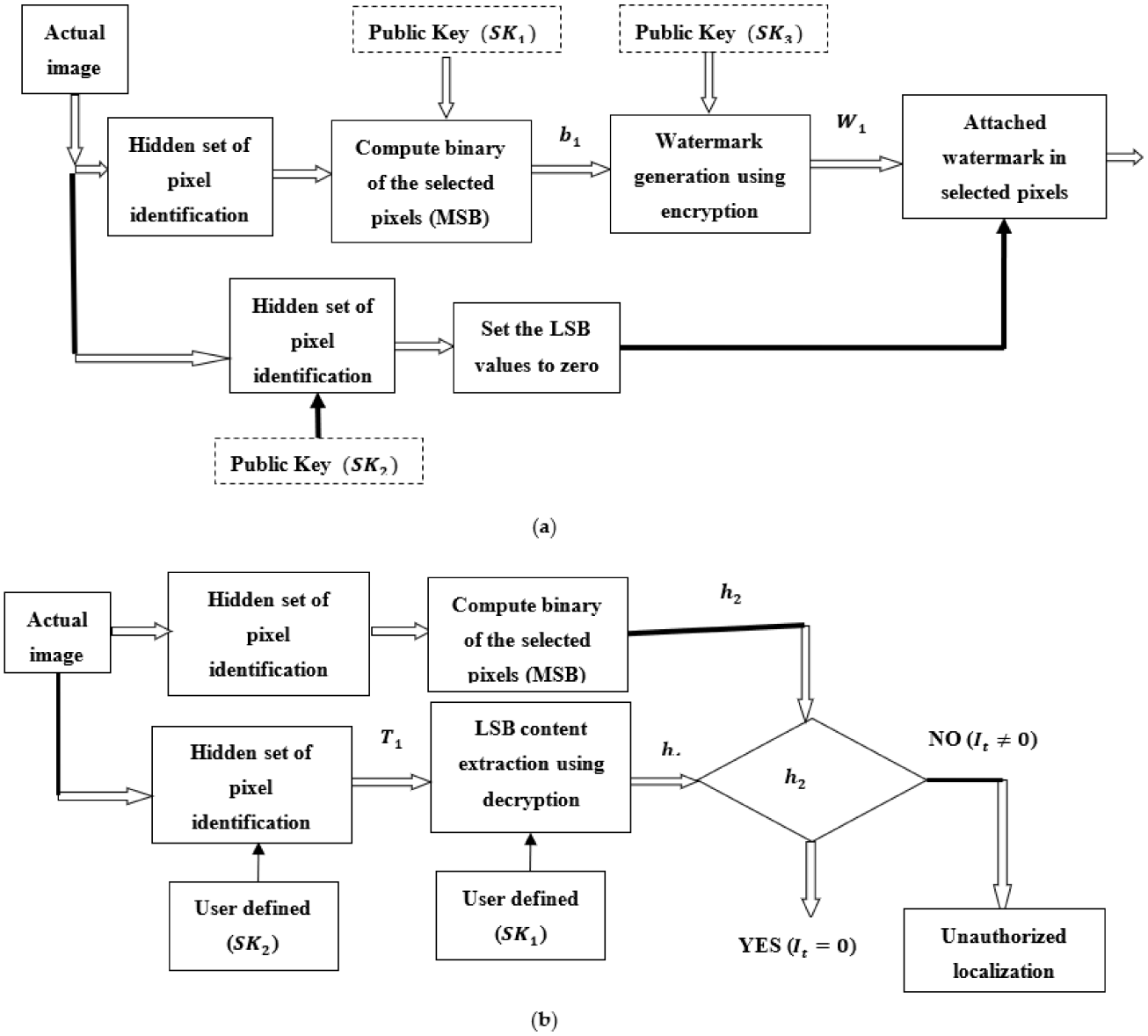

Figure 6. Image authentication using robust watermarking; (**a**) verifier generator; (**b**) authenticity confirmation.

The hash function can be calculated for the public or private key using digital signatures algorithm which can be applied directly to the message for its authentication or its hash value to create a tag used for its verification. this hash function 'H' follows the integer code generation method that arises from the key and generates a value from a text.

it also follows the variables which is a set of information. The digital signature algorithm and has function have same features which is used to compares the signature depends on the dissimulation and selected characteristics [32]. Variable length code can also be assigned to digital signature for its verification. Coefficient quantization applied to obtain $\{0, 1\}$ sequence which can be encrypted to generate electronic signature. Such method logical with 2 & 3 festering degree but bargaining among complexity, safety and processing duration [33]. Cryptography provides higher level solutions for digital image security. Standard cryptology supply severe confirmation rules to decide profile genuine from its binary representation or image pixels changes [34]. This approach has good performance but localizations of the areas that were evaluated are not up to the mark. Detection of tempered image was well using conventional cryptography algorithm approach. The subset of frames represented in Figure 7 under different pose, illumination and may be useful for identification purpose.

Figure 7. Subgroup of structures reflecting the facts introduced in a video. Exclusive pictorial captured image under different illumination, pose and expressions from same occasion where some frames prove to be convenient for profile identification; other may be harmful to performances.

Recognition of video profile demands complement of entire structure available in both pictorial. Although, entire the structures are not likewise instructive and may experience from inequality due to postures, low image quality, illumination and expression. So, some frame might get damaged due presence of covariates and it is very important to choose and employ video information efficiently and carefully [35].

5. Frame Selection and Average Score Algorithm

The algorithm for video image frame selection and its estimated coefficients for maximum average score are discussed in the form of below mentioned steps:

1. Video frame selection based on average using discrete wavelet transform method which firstly identifies the first given input image (I) which may be evaluated as:

$$I(DWT) = \left[I_{ap}, I_{v,h,d}\right]$$

where I_{ap} represents the estimated coefficients of the image, $I_{v,h,d}$ contains coefficient details of vertical, horizontal and verticals sidebands.

2. Filtering process will be applied using high pass and low pass for decomposition of parents wavelets.
3. Next level of DWT now applied to first approximation achieved in first step approximation band.

$$I^I(DWT) = \left[I^I_{ap}, I^I_{v,h,d}\right]$$

where, I^I_{ap}, $I^I_{v,h,d}$ denotes second level estimation of input image (I).

4. Average of every DWT band is evaluated by dividing image in $x \times y$ windows being captured.

$$H(j) = -\sum_{i=1}^{m} P(j_i) log_2 P(j_i)$$

where, $P(j_i)$ is the likelihood majority function which indicates pixel values in probability form reflecting in locality and m is the complete pixels.

5. If window size is $L_x \times W_y$ then

$$P(j_i) = \frac{m_{j_i}}{L_x \times W_y}$$

where, m_{j_i} denotes number of pixels in windows.

6. Average of every opening now integrated to evaluate the attribute merit of line.

$$FH = \sum_{i=1}^{p} (|E_i|)$$

Here, FH indicates feature score value, p is the digit of openings and E_i is the density of the ith windows.

7. Final total score of images I, $FH(I)$ was obtained by averaging the feature value of each band individually:

$$FH(I) = FH\left(I^I_{ap}\right) + FH\left(I^I_{h,v,d}\right) + FH(I_{h,v,d})$$

8. For a video image V_i, feature score of frames (f_i) is denoted by $FH(f_i)$ and obtained max-min normalization using

$$m_{\min} = \frac{FH(f_i) - \min(FH)}{\max(FH) - \min(FH)}$$

where, FH denotes all feature scores for V_i and $\min(FH)$, $\max(FH)$ denotes the denotes the minimum and maximum value of FH.

9. Formerly the outcome of individual structure is evaluated compatible process for structure nomination is carry out to identity best deposit frame [36].

$$\theta_i = 1, \; if \; n_i \geq \sigma_n + \frac{\mu_n}{2}$$
$$0, \text{ otherwise}$$

where, μ_n denote mean appropriate for the feature value and σ_n represents the standard deviation.

10. Testing performed for the rich feature frame from the database and verified with the matched score for its perfect authentication.

The incorrect receiving and incorrect refusal cost is high for feature trained portrayal compared to Eigen, random and normal feature images and for security point of view it must too low to achieve desirable high verification performance. But the false acceptance rate is high of feature trained image which is a good symbol of achieving high verifica-

tion rate and it helps in maintaining the security measures in real time image like video surveillance, authentication etc. depicted in Figures 8 and 9. The actual acceptance can be normalized by decreasing the false acceptance rate or false rejection rate and if it increased it will linearly grow as shown in Figures 8 and 9 below.

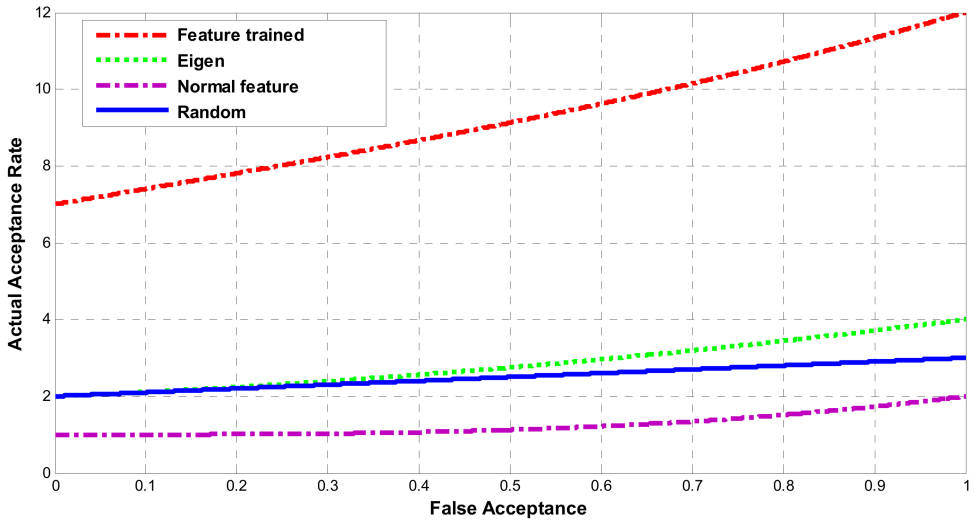

Figure 8. False acceptance rate (FAR).

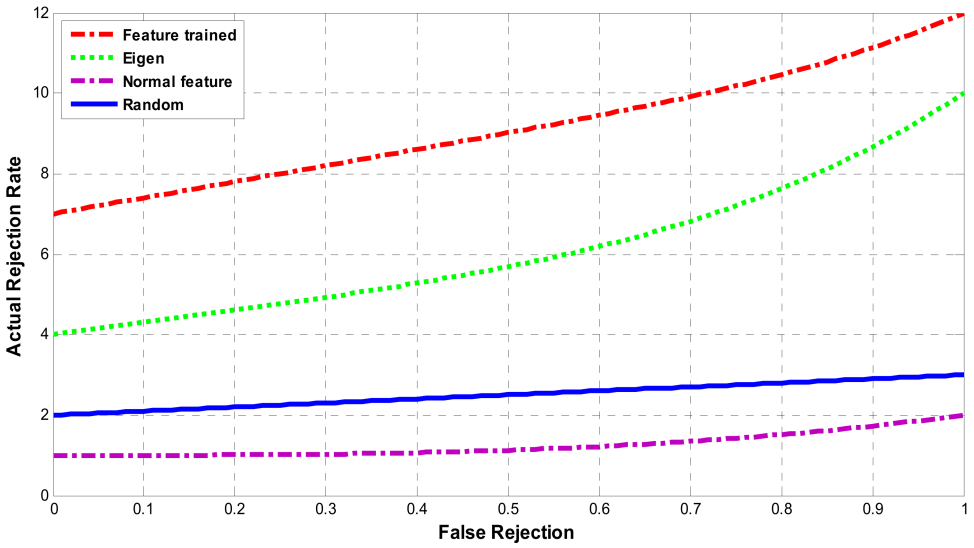

Figure 9. False rejection rate (FRR).

6. Proposed Model for Identification and Verification

The proposed model for face identification and verification is shown in Figure 10 below. This proposed model is used to identify the face succession from the given input and track the identified face over the successive frame and selects the suitable and best face for proper identification with assumption is that background is previously known and fixed. If no any face is detected then system the background by taking information from previous frame. At the final stage of verification phase if newly profile is recognized it will switched to instruction stage for newly profile prototype and if face is identified from the stored face data bank, then analogous profile prototype is re-teach. Based on above proposed model the identification and verification has been performed for the four input images (feature trained, Eigen, random and random) and verification percentage will be keeping the reference of false acceptance rate of above observed results. The real

time images have been captured from the various Utube videos, social networking site etc. including your own database and simulated the result to achieve good performance as discussed in Sections 7 and 8.

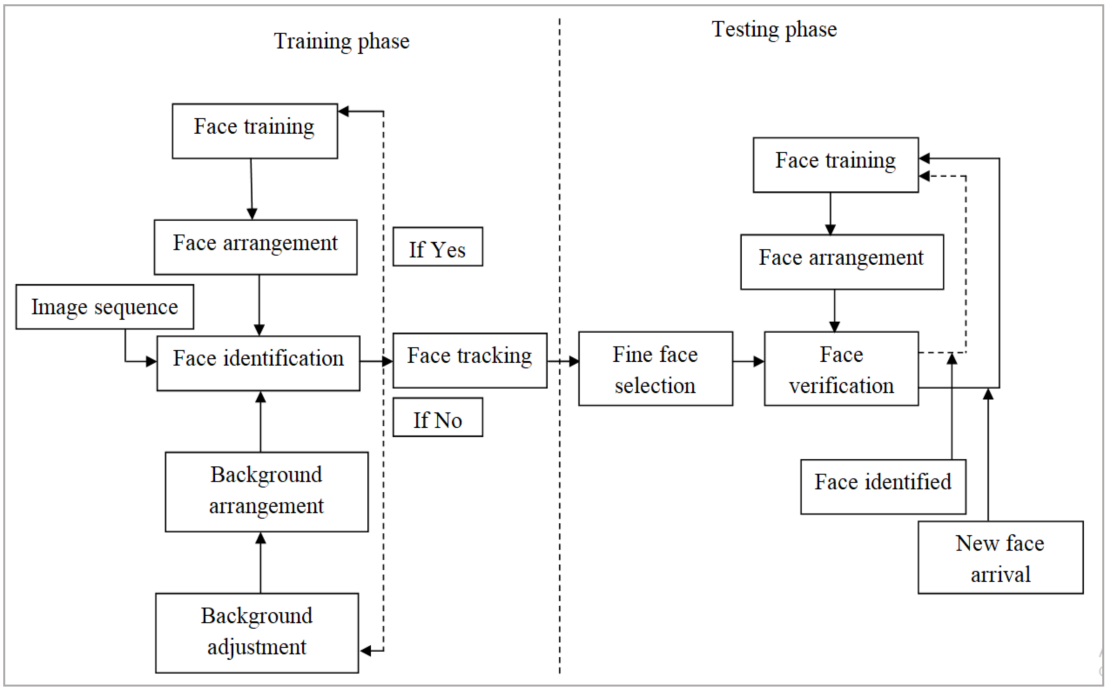

Figure 10. Proposed model for face identification and verification with training and testing stage.

7. Results & Discussions

The experiments are performed with the images gathered from social networking videos including your database which contains 10–100 frames with a duration of 2–6 s having some informative-based features which were firstly trained and tested using the above-proposed model for its verification percentages. We analyze the performance for a stable quantity of structures i.e., unless concerning versatile methods and any frame selection algorithms.

The performance report depicted in Figures 11–14 indicates that feature-trained image accuracy of the different subjects is efficient as compared to Eigen, random and normal feature images. Instagram have much more accuracy compared to other Facebook, Utube and database (self) image the reason might be that it was not tempered and contains all its feature being captured whereas the images of Utube have less accuracy compared to other images. The preliminary score will help to evaluate the overall score of each frame by averaging the score at the maximum level to get desired verification rate. The security level can be improved more by assigning each image with unpredictable coding that has some private key instead of hash coding. The accuracy rate (%) and error with hit rate (%) are mentioned in Tables 1–4 for various databases i.e., own created, Utube, Facebook and Instagram.

Table 1. Database (own created).

Image Type	Identification Accuracy Rate (%)	Verification	
		Error (%)	Hit (%)
1. Random	90.12	9.88	3.65
2. Eigen	91.54	8.64	7.45
3. Feature trained	98.33	1.67	8.43
4. Normal feature	88.89	11.11	2.34

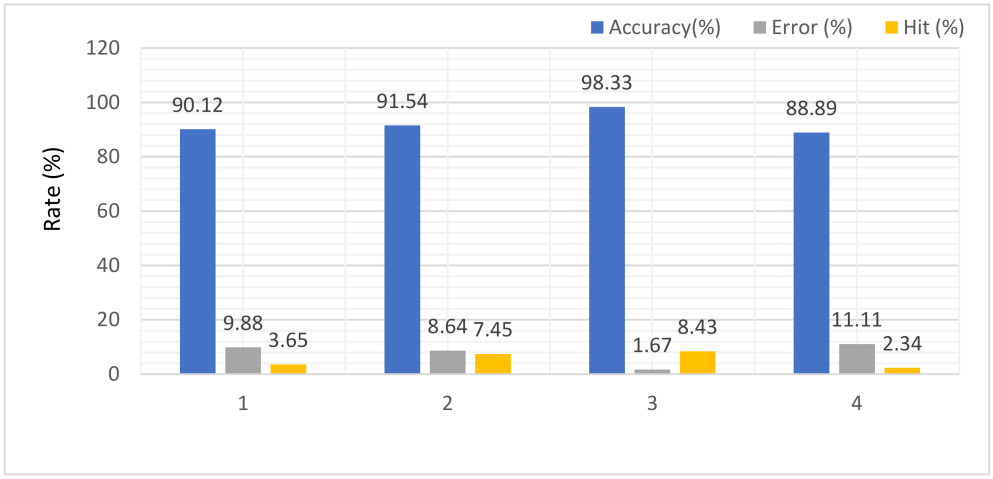

Figure 11. Self-collected images performance from the video.

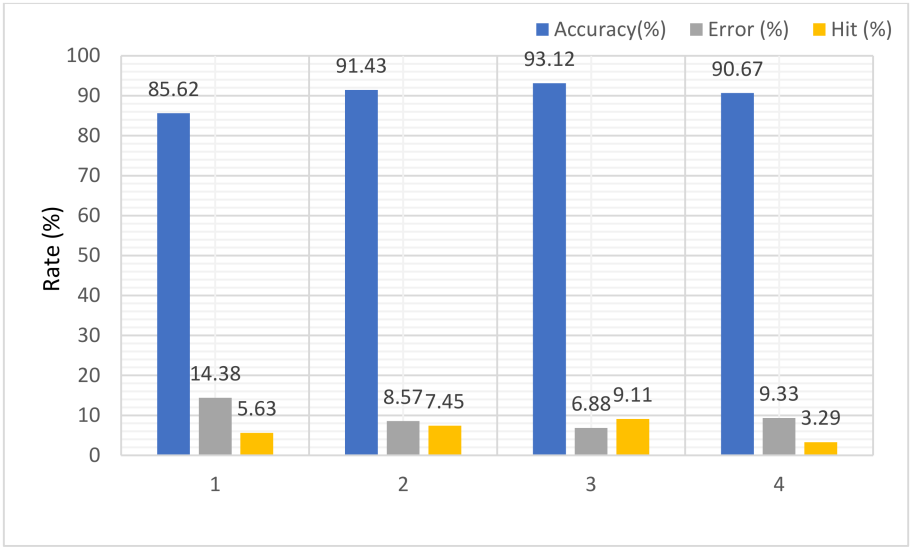

Figure 12. Performance report for Utube video images.

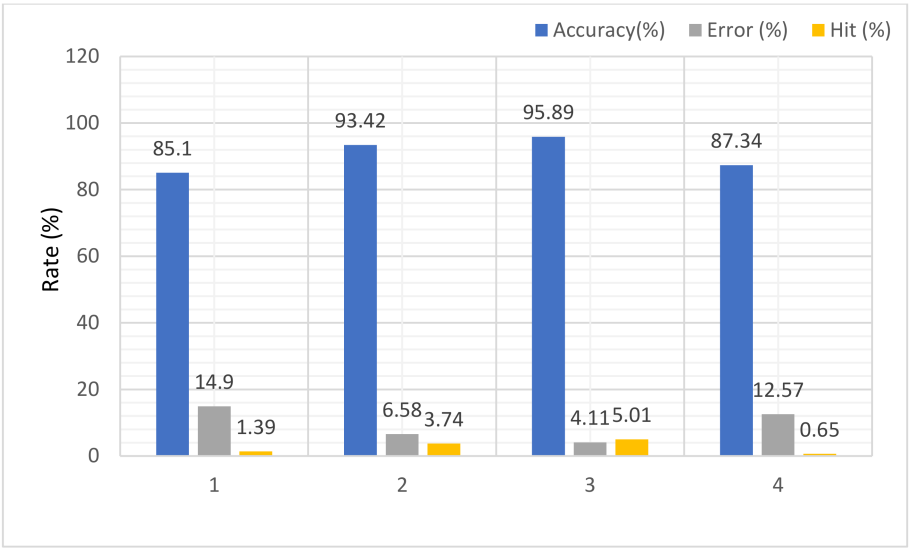

Figure 13. Performance report for Facebook images.

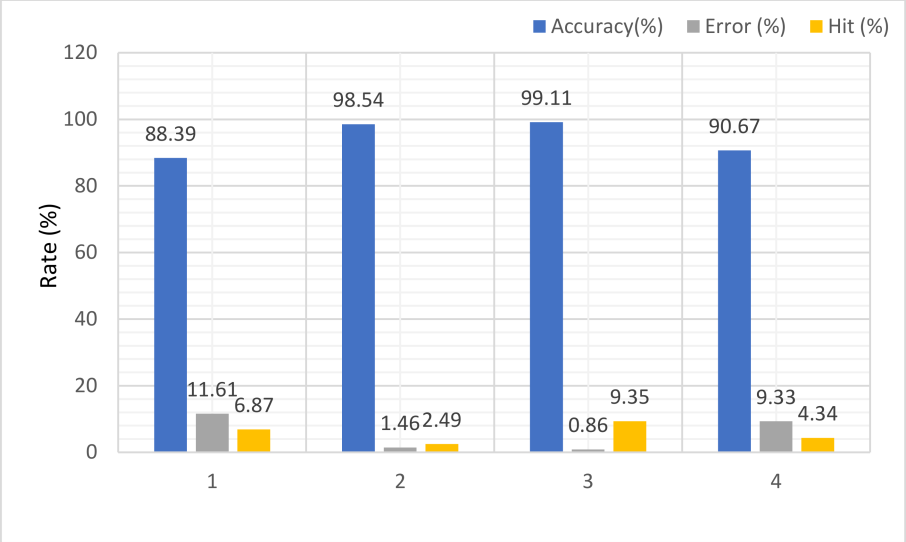

Figure 14. Performance report for Instagram images.

Table 2. Utube (database).

Image Type	Identification Accuracy Rate (%)	Verification	
		Error (%)	Hit (%)
1. Random	85.62	14.38	5.63
2. Eigen	91.43	8.57	7.45
3. Feature trained	93.12	6.88	9.11
4. Normal feature	90.67	9.33	3.29

Table 3. Facebook (database).

Image Type	Identification Accuracy Rate (%)	Verification	
		Error (%)	Hit (%)
1. Random	85.10	14.9	1.39
2. Eigen	93.42	6.58	3.74
3. Feature trained	95.89	4.11	5.01
4. Normal feature	87.34	12.57	0.65

Table 4. Instagram (database).

Image Type	Identification AccuracyRate (%)	Verification	
		Error (%)	Hit (%)
1. Random	88.39	11.61	6.87
2. Eigen	98.54	1.46	2.49
3. Feature trained	99.11	0.86	9.35
4. Normal feature	90.67	9.33	4.34

8. Conclusions

The performance report depicted in above figure indicates that feature trained image accuracy of different subject is efficient as compared to Eigen, random and normal feature images. The Instagram have much more accuracy compared to other Facebook, Utube and database (self) image the reason might be that it was not tempered and contains all its feature being captured whereas the images of Utube have less accuracy compared to other images. Preliminary score will help to evaluate the overall score of each frame and

by averaging the score at maximum level to get desired verification rate. Security level can be improved more by assigning each image with unpredictable coding that have some private key instead of hash coding. Also, validation will be quite easy by evaluating the score value of each frame and it may help to improve the security features. The proposed model can be implemented with embedded HMM using a long video sequnces. Also, the insertion of colour data in the monitoring vector may appreciably improve the performance of the proposed identification and verification model. Face division algorithms that has the ability to cope with different scenarios may provide good approximation.

Author Contributions: Conceptualization, S.U. and M.K. (Mohit Kumar); methodology, S.U., M.K. (Mohit Kumar), S.V. and K.; software, A.U.; validation, M.K. (Mohit Kumar), S.V. and A.S.M.S.H.; formal analysis, K. and A.U.; investigation, M.K. (Maninder Kaur); resources, A.U. and S.S.; data curation, S.S.; writing—original draft preparation, S.U. and S.V.; writing—review and editing, M.K. (Mohit Kumar); visualization, A.U. and S.S.; supervision, I.-H.R. and A.S.M.S.H.; project administration, I.-H.R. and A.S.M.S.H.; funding acquisition, I.-H.R. and A.S.M.S.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Research Foundation of Korea (NRF) 415 Grant by the Korean Government through the Ministry of Science and ICT (MSIT) under Grant 416 2021R1A2C2014333, and Woosong University Academic Research Fund 2023, Korea.

Informed Consent Statement: Written informed consent has been obtained from the patients to publish this paper.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Upadhyay, A.; Sharma, S. Robust Feature Extraction using Embedded HMM for Face Identification & Verification. *Int. J. Appl. Eng. Res.* **2017**, *12*, 15729–15777.
2. Bhatt, H.; Singh, R. On recognizing faces in videos using clustering-based re-ranking and fusion. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 1056–1068. [CrossRef]
3. Begum, M.; Uddin, M.S. Digital image watermarking techniques: A review. *Information* **2020**, *11*, 110. [CrossRef]
4. Abraham, J.; Paul, V. An imperceptible spatial domain color image water scheme. *J. King Saud Univ.-Comput. Inf. Sci.* **2019**, *31*, 125–133.
5. Liu, Y.; Tang, S.; Liu, R.; Zhang, L.; Ma, Z. Secure and robust digital image watermarking scheme using logistic and RSA encryption. *Expert Syst. Appl.* **2018**, *97*, 95–105. [CrossRef]
6. Alsawwaf, M.; Chaczko, Z.; Kulbacki, M. In your face: Person identification through ratios and distances between facial features. *Vietnam J. Comput. Sci.* **2022**, *9*, 187–202. [CrossRef]
7. Mohammed, A.; Kadhim Farhan, A. A novel improvement with an effective expansion to enhance the MD5 hash function for verification of a secure E-Document. *IEEE Access* **2020**, *8*, 80290–80304. [CrossRef]
8. Chambino, L.L.; Silva, J.S.; Bernardino, A. Multispectral facial recognition: A review. *IEEE Access* **2020**, *8*, 80290–80304. [CrossRef]
9. Chen, H.; Shi, B.; Zhong, T. Research on recognition method of electrical components based on YOLO v3. *IEEE Access* **2019**, *7*, 157818–157829. [CrossRef]
10. Bhatti, M.; Khan, M.; Aslam, M.; Fiaz, M.J. Weapon detection in real-time CCTV videos using deep learning. *IEEE Access* **2021**, *9*, 34366–34382. [CrossRef]
11. Fang, W.; Wnag, L.; Ren, P. Tinier-YOLO: A real-time object detection method for constrained environments. *IEEE Access* **2020**, *8*, 1935–1944. [CrossRef]
12. Li, H.; Hu, J.; Yu, J.; Wu, Q. UFaceNet: Research on multitask face recognition algorithm based on CNN. *Algorithms* **2021**, *12*, 268. [CrossRef]
13. Dash, S.; Verma, S.; Kavita; Khan, M.S.; Wozniak, M.; Shafi, J.; Ijaz, M.F. A Hybrid Method to Enhance Thick and Thin Vessels for Blood Vessel Segmentation. *Diagnostics* **2021**, *11*, 2017. [CrossRef]
14. Shenvi, D.; Shet, K. CNN based COVID-19 prevention system. In Proceedings of the 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), Coimbatore, India, 25–27 March 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 873–878.
15. Kumar, M.; Raju, K.S.; Kumar, D.; Goyal, N.; Verma, S.; Singh, A. An efficient framework using visual recognition for IoT based smart city surveillance. *Multimed. Tools Appl.* **2021**, *80*, 31277–31295. [CrossRef]
16. Yang, G.; Jan, M.A.; Rehman, A.U.; Babar, M.; Aimal, M.M.; Verma, S. Interoperability and Data Storage in Internet of Multimedia Things: Investigating Current Trends, Research Challenges and Future Directions. *IEEE Access* **2020**, *8*, 124382–124401. [CrossRef]
17. Li, S.; Jain, A. *Handbook of Face Recognition*; Springer: Secaucus, NJ, USA, 2005.

18. Li, H.P.; Li, J. Implement of Face Recognition System Based on Hidden Markov Model. In Proceedings of the Sixth International Conference on Natural Computation (ICNC), Yantai, China, 10–12 August 2010; IEEE: Piscataway, NJ, USA, 2010.
19. Ali, D.; Touqir, I.; Siddiqui, A.M.; Malik, J.; Imran, M. Face Recognition System Based on Four State Hidden Markov Model. *IEEE Access* **2022**, *10*, 74436–74448. [CrossRef]
20. Dogra, V.; Verma, S.; Kavita; Chatterjee, P.; Shafi, J.; Choi, J.; Ijaz, M.F. A Complete Process of Text Classification System Using State-of-the-Art NLP Models. *Comput. Intell. Neurosci.* **2022**, *2022*, 1883698. [CrossRef]
21. Rani, P.; Kavita; Verma, S.; Rawat, D.B.; Dash, S. Mitigation of black hole attacks using firefly and artificial neural network. *Neural Comput. Appl.* **2022**, *34*, 15101–15111. [CrossRef]
22. Chien, J.T.; Liao, P. Maximum confidence hidden Markov modelling for face recognition. *IEEE Trans. Pattern Mach. Intell.* **2008**, *30*, 312–323. [CrossRef]
23. Kumar, M.; Verma, S.; Kumar, A.; Ijaz, M.F.; Rawat, D.B. ANAF-IoMT: A Novel Architectural Framework for IoMT-Enabled Smart Healthcare System by Enhancing Security Based on RECC-VC. *IEEE Trans. Ind. Inform.* **2022**, *18*, 8936–8943. [CrossRef]
24. Pradhan, N.R.; Singh, A.P.; Verma, S.; Wozniak, M.; Shafi, J.; Ijaz, M.F. A blockchain based lightweight peer-to-peer energy trading framework for secured high throughput micro-transactions. *Sci. Rep.* **2022**, *12*, 14523. [CrossRef] [PubMed]
25. Kumar, M.; Mukherjee, P.; Verma, S.; Kaur, M.; Singh, S.; Kobielnik, M.; Woźniak, M.; Shafi, J.; Ijaz, M.F. BBNSF: Blockchain-Based Novel Secure Framework Using RP2-RSA and ASR-ANN Technique for IoT Enabled Healthcare Systems. *Sensors* **2022**, *22*, 9448. [CrossRef] [PubMed]
26. Marvel, L.M.; Hartwig, G.W. Compression compatible fragile and semi fragile tamper detection. In Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents, San Jose, CA, USA, 9 May 2000; Volume 2, pp. 3971–3981.
27. Fridrich, J.; Goljan, M.; Du, R. Invertible authentication. In Proceedings of the SPIE, Security and Watermarking of Multimedia Contents, San Jose, CA, USA, 20–26 January 2001; pp. 23–26.
28. Mun, H.; Han, K. Design for access control system based on voice recognition for infectious disease prevention. *J. Korea Converg. Soc.* **2020**, *11*, 19–24.
29. Lee, M.; Mun, H. Comparison analysis and case study for deep learning-based object detection algorithm. *Int. J. Adv. Sci. Converg.* **2020**, *2*, 7–16. [CrossRef]
30. Gupta, R.; Verma, E.S.; Kavita, E. Solving ipv4 (32 bits) address shortage problem using ipv6 (128 bits). *IJREISS* **2012**, *2*, 58–68.
31. Sharif, M.; Shah, J.H.; Mohsin, S.; Raza, M. Sub-Holistic Hidden Markov Model for Face Recognition. *Res. J. Recent Sci.* **2013**, *2*, 10–14.
32. Kumar, M.; Kumar, D.; Akhtar, M.A.K. A modified GA-based load balanced clustering algorithm for WSN: MGALBC. *Int. J. Embed. Real-Time Commun. Syst. (IJERTCS)* **2021**, *12*, 44–63. [CrossRef]
33. Londhe, A.; Rao, P.V.R.D.; Upadhyay, S.; Jain, R. Extracting behavior identification features for monitoring and managing speech dependent smart mental illness healthcare systems. *Comput. Intell. Neuro Sci.* **2022**, *2022*, 8579640. [CrossRef]
34. Ghosh, G.; Verma, S.; Jhanjhi, N.Z.; Talib, M.N. Secure Surveillance System Using Chaotic Image Encryption Technique. *IOP Conf. Ser. Mater. Sci. Eng.* **2020**, *993*, 012062. [CrossRef]
35. Barr, J.; Bowyer, K.; Flynn, P. Effective and ineffective digital watermarks. *Commun. ACM* **1998**, *41*, 31–33.
36. Kumar, A.; Kumar, M.; Verma, S.; Jhanjhi, N.Z.; Ghoniem, R.M. Vbswp-CeaH: Vigorous Buyer-Seller Watermarking Protocol without Trusted Certificate Authority for Copyright Protection in Cloud Environment through Additive Homomorphism. *Symmetry* **2022**, *14*, 2441. [CrossRef]