Information Security Journal: A Global Perspective

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/uiss20

Multifactor authentication system based on color visual cryptography, facial recognition, and dragonfly optimization

D. R. Ibrahim, J. S. Teh & R. Abdullah

To cite this article: D. R. Ibrahim, J. S. Teh & R. Abdullah (2021) Multifactor authentication system based on color visual cryptography, facial recognition, and dragonfly optimization, Information Security Journal: A Global Perspective, 30:3, 149-159, DOI: 10.1080/19393555.2020.1817633

To link to this article: https://doi.org/10.1080/19393555.2020.1817633

Published online: 12 Sep 2020.

INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE
2021, VOL. 30, NO. 3, 149–159
https://doi.org/10.1080/19393555.2020.1817633

Taylor & Francis
Taylor & Francis Group

Multifactor authentication system based on color visual cryptography, facial recognition, and dragonfly optimization

D. R. Ibrahim[a], J. S. Teh[b], and R. Abdullah[a,b]

[a]National Advanced IPv6 Centre, Universiti Sains Malaysia, George Town, Malaysia; [b]School of Computer Sciences, Universiti Sains Malaysia, George Town, Malaysia

ABSTRACT
Facial recognition as an authentication factor requires that facial images and features are tamper-free. Visual cryptography (VC) is commonly used for this purpose but leads to additional computational overhead and lower recognition accuracy. To address these issues, we propose a multifactor authentication (MFA) system based on facial recognition that uses VC to secure biometric data, and also as a second authentication factor. The shares generated by VC are used as authentication tokens. These tokens are verified by the same facial recognition algorithm used to recognize a live facial image of the user. This simple albeit novel approach leads to lower computational cost because the same algorithm can be used to verify both authentication factors. To maximize verification accuracy, the binary dragonfly optimization algorithm is used to maximize the quality of the recovered image from VC, as well as the accuracy of the facial recognition algorithm itself through feature selection. The combination of these separate ideas leads to a novel MFA system that is efficient and highly accurate. Experimental verification based on various face image databases depicts the proposed system's security, efficiency, and near-ideal recognition accuracy of up to 99.81%.

KEYWORDS
Authentication; biometrics; facial recognition; multifactor authentication; visual Cryptography

1. Introduction

In today's digital world, data security is of utmost importance. A multitude of mechanisms has been proposed to ensure that confidential data remains private, and only authorized individuals would have the permission to access them (A. K. Sangaiah et al., 2019). Single-factor authentication (SFA) is one of the simplest ways to secure access to a system or data. As its name implies, SFA involves the use of only one factor, which can include knowledge (something the user knows), possession (something the user has) or inherence (something the user is). The implementation of these factors can include the use of passwords, credit cards, smart cards, encryption algorithms, or biometrics (Mwema et al., 2015).

However, each one of these singular factors has their own limitations. For example, passwords can be forgotten or guessed, cards can be stolen or misplaced and biometric templates can be subject to tampering. Some biometrics such as DNA need expensive equipment while others such as fingerprint or iris have low accuracy (Ibrahim et al., 2017). Combining these factors can circumvent their individual shortcomings, which led to the development of multifactor authentication (MFA) systems. MFA generally outperform their SFA counterparts in terms of efficiency, accuracy, and security. As such, MFA are widely used solutions for users to protect their high risk, sensitive information (Abhishek et al., 2013; Ibrahim et al., 2019). A true MFA system requires the use of two or more different categories of authentication factors. Using multiple factors from the same category would not constitute MFA (Mohammed & Yassin, 2019). Common applications of MFA include ATM cash withdrawals which require ATM cards (tokens) and passwords, and e-wallets that require additional one-time passcodes sent to mobile phones for login purposes (Steam Guard Mobile Authenticator, 2017). The general public is also well aware of the importance of MFA. For example, in Europe, 73% of Visa's customers see that the use of at least two factors for authentication is a necessity (European consumers ready to use biometrics for securing payments, 2016). The use of MFA spans across commercial, governmental, and forensic applications (Ometov et al., 2018).

CONTACT J. S. Teh jesen_teh@usm.my National Advanced IPv6 Centre, Universiti Sains Malaysia, George Town, Malaysia

The face is one of the most common biometric modalities. Facial recognition (FR) is considered a non-intrusive method as it does not need physical interaction. However, it has lower accuracy as compared to other biometric modalities such as fingerprint or iris due to the high dimensionality of extracted features and uncontrolled conditions such as pose, expression, illumination which affects the intra-personal and inter-personal variations (Cai et al., 2015). Thus, suitable approaches for feature selection should be included if FR is used as part of an MFA system. In addition, the use of FR must also involve biometric template protection (BTP) to ensure privacy and avoid misuse of biometric data. As such, the performance and security of an authentication system that relies on FR is also dependent on the BTP scheme being implemented. Current BTP schemes still require improvements in terms of security, performance, and privacy (Sandhya & Prasad, 2016).

In the proposed work, we introduce a novel way of utilizing VC and FR for MFA. Unlike past work that uses VC only for biometric template protection, we use the VC shares itself as an authentication factor. The trained FR algorithm is then used to recognize both the VC recovered image and the user's live facial image. This leads to lower computational cost because FR is used to verify both two authentication factors and is near-instantaneous. The use of dragonfly optimization is important to maximize the quality of the VC's recovered image and the accuracy of the FR algorithm, which leads to higher authentication accuracy. VC will first encrypt facial images, decomposing them into two shares. One of these shares will be kept by the user as a token for authentication while the other will be stored by the system. Face images of the user will be used to train an FR algorithm. The trained FR algorithm will be used for authentication by first recognizing the recovered face image obtained by overlapping the user and system's shares. The same FR algorithm will then attempt to recognize a *live* face image of the user that is taken on-the-fly. An individual is authenticated if both the recovered and live images are recognized successfully. Although the enrollment process for the system is slightly more complex as it involves capturing user face images for training purposes and to produce the shares, the resulting system is fast, accurate, easy to use, non-intrusive and secure.

The rest of this paper is organized as follows: Section 2 discusses recent work involving secret-sharing schemes and VC in MFA, providing rationale for the proposed work. Section 3 discusses the individual algorithms (optimization, visual cryptography) before the overall MFA system is outlined in Section 4. Experimental results and analyses are reported in Section 5 before the paper is concluded in Section 6.

2. Related work

VC has generally been used to secure biometric templates. However, there is a lack of MFA systems that utilize VC in recent literature. Thus, we expanded the coverage of related work to include MFA systems that utilize conventional secret-sharing schemes. An MFA system utilizing VC was proposed by Suryadevara et al. (2011). Rather than conventional biometric modalities, the human tongue was used. Due to the unique characteristics of the human tongue, the proposed system has good security properties. Although recognition accuracy was not reported, the VC scheme being used has a pixel expansion factor of 2, leading to share images and recovered images with twice the size of the original secret image. This results in a loss in contrast, which should theoretically affect recognition accuracy. Another MFA scheme using VC was proposed by Judith et al. (2016). They used proposed an MFA system based on three biometric modalities: iris, face, and fingerprint. The goal of using multiple modalities is to improve data security and deter intruders. Every biometric template is encrypted using VC into three shares. These shares are recombined when authenticating users. Although the use of multiple biometric modalities is supposedly more secure, the use of visual cryptography on three different templates leads to lower accuracy and efficiency.

As for MFA schemes based on conventional secret sharing, Venukumar and Pathari (2016) used threshold secret sharing (TSS) to generate multiple one-time passwords (OTP) based on a user-supplied PIN or password. TSS is a method commonly used in industrial environments (A. K. Sangaiah, Medhane et al., 2020). The OTPs are sent to multiple devices, which are all required to be sent back to the server for recombination. Apart from being less user friendly, the proposed system still has a dependence on passwords which are susceptible to brute-force attacks and misuse. Battalglia et al. (2014) proposed a face-recognition scheme based on a secret-sharing concept in which different facial features of the user were only partly stored in an RFID tag, avoiding the security concern of having the complete biometric data stored in the repository being stolen. Lin et al. (2018) proposed a facial recognition model for user identification in public transportation systems based on secret sharing and the nearest neighbor (NN) algorithm. Their scheme guarantee privacy protection even when facial features are stored in a distributed manner. Their scheme achieved a recognition percentage of approximately 95.7%.

In the proposed MFA system, we improve upon existing work in several aspects. First, without the use of passwords as an authentication factor, user friendliness of the system is improved, and removes risks attributed to user errors. Secondly, by using an optimization algorithm, we attempt to maximize the recognition accuracy to be as near-ideal as possible. High recognition accuracy is also facilitated by the use of the optimized VC algorithm that has no pixel expansion. Finally, we maximize the efficiency of the recognition process by moving the bulk of computational work to the pre-processing (enrollment) phase, thus making the proposed MFA system suitable for practical applications. In Table 1 we provide a brief comparison of the proposed work and the related ones in this section.

Table 1. Comparison of MFA based on VC and secret sharing.

Method	Biometric Modality	Template Security	Accuracy (%)
Proposed work	Face	VC	99.81
Suryadevara et al. (2011)	Tongue	VC	-
Venukumar and Pathari (2016)	None (Password-based)	Threshold VC	-
Judith et al. (2016)	Iris, face and fingerprint	VC	45
Lin et al. (2018)	Face	Secret-Sharing	98
Battalglia et al. (2014)	Face	Secret-Sharing	97.69

3. Preliminaries

The proposed MFA system involves the use of VC and FR for authentication. Thus, the performance of the overall system is dependent on each of these individual algorithms. In order to maximize performance, we utilize BDA to select optimal parameters for VC and optimal features for FR. This section delves into vital details about BDA as well as our optimized implementations for VC and FR.

3.1. Binary dragonfly algorithm

Heuristic-based approaches (such as the dragonfly algorithm) are used to identify solutions to problems that cannot be solved in polynomial time (A. K. Sangaiah, Hosseinabadi et al., 2020). The dragonfly algorithm is an optimization algorithm based on the swarming behavior of dragonflies which can be static or dynamic. These behaviors are analogous to exploration and exploitation in metaheuristics (Mirjalili, 2015). The six parameters of BDA include

$$Separation, S_i = -\sum_{j=1}^{N}(X_i - X_j), \tag{1}$$

$$Alignment, A_i = \frac{\sum_{j=1}^{N} V_j}{N}, \tag{2}$$

$$Cohesion, C_i = \frac{\sum_{j=1}^{N} X_j}{N} - X_i, \tag{3}$$

$$Attraction, F_i = X^{+} - X_i, \tag{4}$$

$$Distraction, E_i = X^{-} + X_i, \tag{5}$$

where X_i, X_j, X^{+}, X^{-} refer to positions of the current dragonfly, j^{th} dragonfly, food source, and enemy, respectively, and t denotes the number of iterations. To update the position of dragonflies in a search space and formulate their movements, two vectors are considered. The step vector (direction of dragonfly movement) is calculated as

$$\Delta X_{t+1} = (sS_i + aA_i + cC_i + fF_i + eE_i) + w\Delta X_t, \tag{6}$$

whereas the position vector is calculated as

$$X_{t+1} = X_t + \Delta X_{t-1} \tag{7}$$

To further enhance dragonfly randomness, we calculate

$$X_{t+1} = X_t + \left(0.01X_t \times \frac{r_1 \times \alpha}{|r_2|^{\frac{1}{\beta}}}\right) \tag{8}$$

where r_1, r_2 denote two random numbers in [0,1], $\beta = 1.5$ and α are calculated as

$$\alpha = \left(\frac{\Phi(1+\beta) \times sin(\frac{\pi\beta}{2})}{\Phi(\frac{1+\beta}{2}) \times \beta \times 2^{(\frac{\beta-1}{2})}}\right)^{\frac{1}{\beta}} \tag{9}$$

where $\Phi(x) = (x-1)!$. The probability of dragonfly position changes is calculated using the transfer function

$$T(\Delta x) = \left|\frac{\Delta x}{\sqrt{\Delta x^2 + 1}}\right|. \tag{10}$$

Finally, the position of search agents in the binary search spaces is calculated as

$$X_{t+1} = \begin{cases} \neg X_t & r < T(\Delta x_{t+1}) \\ X_t, & r \leq T(\Delta x_{t+1}), \end{cases} \tag{11}$$

where r denotes a number in the interval of [0,1]. Further details about BDA can be found in the paper by Mirjalili (2015). The simplified BDA pseudocode is shown in Algorithm 1.

Algorithm 1 Dragonfly Algorithm

```
    Initialize the population of dragonflies $X_i$ where $i = \{1, 2, \ldots, n\}$
    Initialize step vectors $\Delta X_i$ where $i = \{1, 2, \ldots, n\}$
    **while** the end condition is not satisfied
    Calculate the objective values of all dragonflies
    Update the food source and enemy
    Update $w, s, a, c, f,$ and $e$ values
    Calculate $S, A, C, F,$ and $E$ values (Eq. 1–5)
    Update step vectors (Eqs. 6–9)
    Calculate probabilities of changing position for all dragonflies (Eq. 10)
    Update position vectors (Eq. 11)
    **end while**
```

3.2. Optimized visual cryptography scheme

VC is a cryptographic technique for image-based secret sharing. Conventionally, encryption and decryption processes can be carried out without mathematical operations by printing shares on transparencies (Naor & Shamir, 1995). Hou (2003) later proposed CVC, which encrypts colored images. However, CVC has drawbacks such as pixel expansion and poor contrast. Pixel expansion refers to the number of sub-pixels in the share image that represents the pixel in the original image in the encryption method. Pixel expansion leads to reconstructed images with poor quality that are larger than the original image. Thus, one of the goals of CVC designs is to minimize pixel expansion. Poor contrast is the other problem in CVC. Contrast refers to the difference in intensity between a black and white pixel in a target image. The contrast must therefore be as large as possible. Both of these parameters (pixel expansion and contrast) affect the quality of the CVC method from the security and performance perspectives. Since the proposed MFA system relies on the performance of CVC as one of its authentication factors, we utilize BDA to optimize the CVC scheme's performance. The optimized CVC method is shown in Figure 1.

The proposed CVC approach has a pixel expansion of 1, which implies that the recovered image is of the same size as the original image. Thus, it is easier for FR to authenticate individuals based on their recovered image. In addition, the quality of encryption is improved. This leads to higher accuracy and security of the overall MFA system.

First, the secret image is divided into three channels (R, G, B) in the color decomposition step, separating the basic matrix of the original image into three matrices. The decomposed matrices are

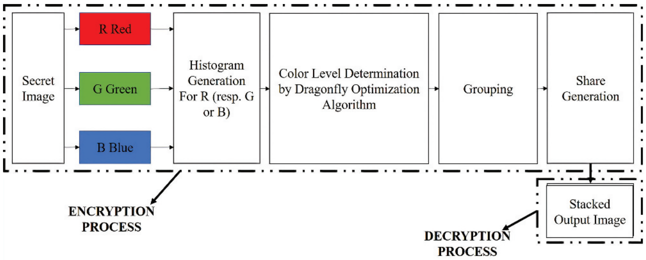

Figure 1. Binary dragonfly algorithm-optimized color visual cryptography .

of the same size as the secret image. After color decomposition, the histograms for each color channel are generated. These histograms depict the intensity distribution of each color channel. We then use BDA to determine the color levels that are used in the encryption process. In other words, BDA is used to determine the number of intensity levels for each channel that minimizes the PSNR and correlation coefficient (CC) which are calculated by comparing original images with their share images. Low PSNR and CC values imply that the original image and share images are entirely different. This in turn implies high security and quality of encryption. BDA is employed for each color channel individually. A total of 1000 iterations are performed to identify the optimal color levels.

Finally, the output from this process is the share images. In the proposed MFA system, one share will be held by the user as token whereas the other will be stored in the system. The share generation process is applied individually on each color channel and is based on the scheme by Naor and Shamir (1995). The decryption process is carried out by just digitally stacking or overlapping the shares on top of each other to recover the original secret image.

3.3. Optimized facial recognition algorithm

The facial recognition algorithm plays an important role as it will be used to verify the validity of both authentication factors, the recovered image from CVC and the user's *live* facial image. First, we use a Gaussian filter to pre-process images to avoid problems caused by noisy images (Sakaue & Shakunaga, 2005, 2006). We implement the filter using MATLAB's computer vision toolbox. Image pre-processing ensures that the face images are relatively independent of various image variations such as lighting, translation, and rotation as shown in Figure 2.

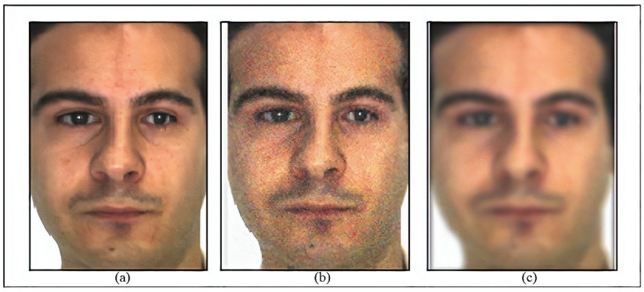

Figure 2. Gaussian filter (a) Original image, (b) Noise detection, (c) Post-filter.

Next, we perform feature detection and extraction. For feature extraction, we use uniform local binary pattern (ULBP), which is widely used for pattern recognition problems (Nanni et al., 2012; Nanni & Lumini, 2008). ULBP extracts the most discriminating features from human face images. The extracted ULBP features are invariant to illumination effects, pose, expression, and age (Chengeta & Viriri, 2018). First, we compute LBP for each pixel (x_c, y_c) as

$$LBP_{(P,R)}(x_c, y_c) = \sum_{p=0}^{p=P-1} S(g_p - g_c)2^P, \tag{12}$$

$$s(g) = \begin{cases} 1, & if\ g \geq 0 \\ 0, & otherwise, \end{cases} \tag{13}$$

where g_c is the gray value of the pixel at x_c, y_c, and P is the number of pixels in the neighborhood of radius R. A subset of these 2^P binary patterns, known as uniform patterns, have at most two transitions from 0 to 1 (or vice versa). The number of output labels generated by mapping patterns of p bits is $p(p-1)+3$. ULBP is then mathematically defined as

$$LBP^{u2}_{P,R}(x_c, y_c) = \begin{cases} I(LBP_{P,R}(x_c, y_c)), & if\ \ U(LBP_{P,R}) \leq 2 \\ P(P-1)+2, & otherwise, \end{cases} \tag{14}$$

where $I(z) \in [0, P(P-1)+1]$ and

$$U(LBP_{P,R}) = S(g_{P-1} - g_c) - S(g_0 - g_c) + \sum_{1}^{P} |S(g_P - g_c) - S(g_{P-1} - g_c)|. \tag{15}$$

$U(LBP_{P,R})$ refers to the number of spatial bitwise transitions (1/0 changes) of a given pattern. For values of $U(LBP_{P,R}) < 2$, pixels are labeled by an index function $I(Z)$. Otherwise, pixels will be assigned values of $(P-1)P+2$. The uniform patterns are indexed by the function $I(Z)$ which contains $(P-1)P+2$ indices (Abhishek et al., 2013). The global high-dimensional feature descriptor is then generated by concatenating all the features.

Finally, for facial recognition, the proposed method uses K-nearest neighbor (KNN) due to its low computational complexity and high accuracy (A. K. Sangaiah et al., 2019; Kumar et al., 2011). BDA is used to select the best features, filtering out irrelevant, noisy, and redundant features. Features which have been identified are used as inputs KNN. The resulting recognition accuracy is used as the fitness function. Features that lead to the highest accuracy will be selected for facial recognition purposes. This step is summarized in Algorithm 2.

```
Algorithm 2 Feature Selection Process
    1. Assign a class label to each individual in the dataset, $P_1, P_2, \ldots, P_n$
    2. Initialize BDA parameters
    3. Train the KNN algorithm and compute its accuracy
    4. Execute Algorithm 1(BDA)
    5. Repeat Step 3 until stopping conditions are satisfied or max iterations
```

The optimized algorithm displayed significant performance improvements. Reduction of the features from feature selection leads to improved accuracy (by preventing overfitting) and improved time complexity. The receiver operating characteristics (ROC) plot for the optimized FR approach is shown in Figure 3. The plot shows that the area under the ROC curve (AUC) is very high at 87%. In addition, the true positive rate (TPR) and false-positive rate (FPR) are close to 1 and 0, respectively. This showcases the accuracy of the optimized FR algorithm. Furthermore, we also compare the proposed work against other recently proposed approaches based on recognition rate as shown in Table 2.

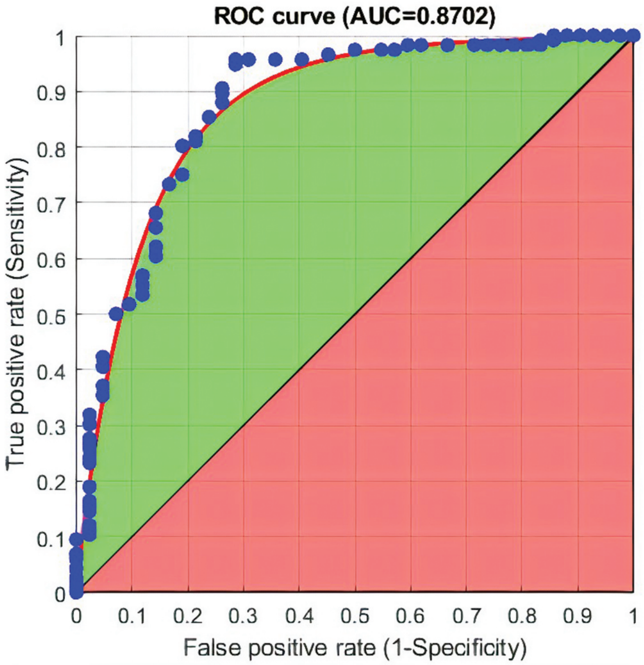

Figure 3. Receiver operating characteristics curve.

4. Proposed multifactor authentication system

The proposed MFA architecture is shown in Figure 4. One of the strengths of the proposed system is that one of the authentication factors (the share images generated by VC) also plays a significant role in securing biometric data. In addition, the same facial recognition algorithm is used for both authentication factors (recovered image and *live* image), lowers the cost of implementation. BDA is used to select optimal features for FR and to select optimal color levels for VC. This maximizes the authentication accuracy two-fold: First, the facial recognition algorithm itself is trained only with optimal facial features to prevent under or overfitting. Second, the quality of the recovered images (after combining image shares) is improved. Improving the quality of the recovered images leads to improved recognition rate as there is less noise in the face images. The steps involved in the proposed MFA system are as follows:

Step 1: Enrollment process. In this step, face images are captured to train the facial recognition algorithm. One of these images is then selected to be encrypted using VC, thus decomposing it into two shares. One of these shares will be stored by the system whereas the other is held by the user as a token. This can be done by printing it onto or even digitally storing it in a smart card.

Step 2: Authentication process. The authentication process has two steps. First, decryption is performed by digitally or physically overlapping two shares to recover the original image. The recovered image is then fed into the trained FR algorithm. If a match is detected, a *live* face image of the user will be taken. The face image is also fed into the FR algorithm. If the user is recognized successfully

Table 2. Comparison of facial recognition approaches.

Algorithm	ORL	AR	LFW
Proposed work (BDA-KNN)	99.90%	99.85%	99.86%
Singh and Chhabra (2018)	99.80%	–	–
Vinay et al. (2017)	95.43%	98.8%	83.37%

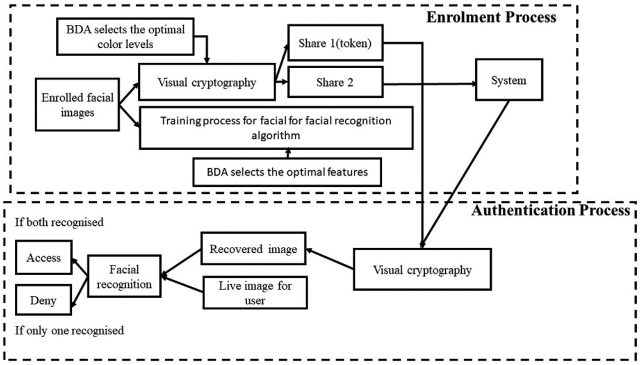

Figure 4. Multifactor authentication architecture.

a second time, the user is considered to be an authentic or valid user.

5. Experimental evaluation

The proposed work is implemented using MATLAB 2018a. We first evaluate the security strength of the first authentication factor by analyzing the differences between the original image and share images. We also provide a discussion on how the proposed MFA system is resistant to several attack scenarios. Finally, we perform experiments on various face image datasets to determine the efficiency and accuracy of the overall MFA system. The AR (Martinez & Benavente, n.d.), LFW (Huang et al., n.d.), FERET (P. P. Phillips et al., 2000), and GBU (P. J. P. J. Phillips et al., 2012) databases were used to evaluate the proposed MFA system. In addition, we also included a custom face database, as sample of which is shown in Figure 5. The custom face database was captured under actual uncontrolled conditions, and includes 9 subjects with 44 images each. In total, there are 396 for 9 subjects. Each image in these datasets has the resolution of 256 × 256 pixels.

5.1. Security

Current MFA systems that require users to expose their secrets in a public place are a fundamental mistake, and is practised every day in millions of transactions around the world. The proposed system effectively removes the security risk involved in using secrets in public for authentication by using CVC to decompose the aforementioned secrets. This results in the first authentication factor. We evaluate the first authentication factor by comparing the entropy of the original, E_o and share images, E_s. Entropy is calculated as

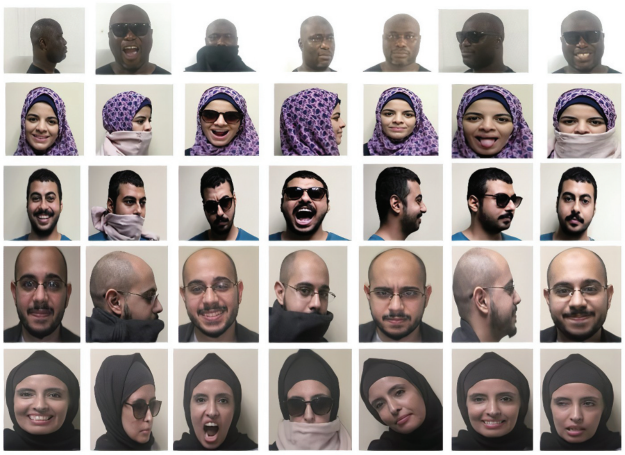

Figure 5. Custom face dataset.

$$E(x) = \sum_{i=1}^{C-1} P(x_i) \log_2 P(x_i) \qquad (16)$$

where $P(x_i)$ is the discrete probability function, x_i are pixel values that range between [0,255], and $C = 256$ is the color level. We calculate entropy values for 10 images (10 individuals) from all five datasets, the results of which are shown in Table 3. We can see that all the share images have near-ideal entropy values (close to 8) as compared to their original images. This implies that the first authentication factor is resistant to entropy-based attacks because the original and shared images are completely different.

Next, the correlation coefficient (CC) between the original and share images is computed as

$$CC(A,B) = \frac{cov(A,B)}{\sqrt{var(A)\sqrt{var(B)}}}, \qquad (17)$$

where A and B denote the secret and share images, respectively. We calculate CC for 10 images from each dataset and tabulated them in Table 4. For all images, the CC between original and share images is close to zero. This implies that there is no identifiable statistical relationship between the images.

We take a look at several possible scenarios where an adversary can attack the proposed MFA system. If an adversary uses a fake share and tries to access the system, the decryption of the share will fail. This is due to the security of VC itself. In the scenario whereby an

Table 3. Entropy analysis for first authentication factor.

Dataset	AR		FERET		LFW		GBU		Custom	
Image	E_o	E_s	E_o	E_s	E_s		E_o	E_s	E_o	E_s
1	7.7640	7.9987	7.7644	7.9989	7.7718	7.9989	7.7702	7.9997	6.7256	7.9989
2	7.7070	7.9990	7.7787	7.9896	7.7767	7.9998	7.7644	7.9991	7.7767	7.9896
3	7.7719	7.9890	7.7734	7.9950	7.7774	7.9953	7.7741	7.9944	7.7788	7.9984
4	7.7755	7.9896	7.7719	7.9990	7.7064	7.9990	7.7711	7.9920	6.7256	7.9988
5	6.7070	7.9989	7.7760	7.9896	7.7773	7.9984	7.7744	7.9645	7.7744	7.9850
6	6.7643	7.9989	7.7770	7.9896	7.7050	7.9990	7.7824	7.9829	7.7720	7.9989
7	7.7643	7.9989	7.7762	7.9889	6.7776	7.9980	7.7711	7.9932	7.7721	7.9931
8	7.7708	7.9985	7.7760	7.9989	6.7091	7.9990	7.7767	7.9923	7.7754	7.9959
9	7.7090	7.9986	7.7676	7.9887	7.7660	7.9940	6.7708	7.9990	7.7719	7.9988
10	7.7785	7.9996	7.7660	7.9998	7.7753	7.9991	6.7256	7.9897	X	X
Average	**7.7653**	**7.9957**	**7.7780**	**7.9939**	**7.7755**	**7.9985**	**7.7780**	**7.9888**	**7.7792**	**7.9996**

Table 4. Correlation coefficient analysis for first authentication factor.

Image	AR	FERET	LFW	GBU	Custom
1	0.006	0.005	0.006	0.002	0.002
2	0.005	0.004	0.006	0.003	0.003
3	0.005	0.004	0.005	0.006	0.004
4	0.004	0.005	0.004	0.006	0.005
5	0.003	0.002	0.004	0.006	0.003
6	0.002	0.003	0.005	0.004	0.002
7	0.002	0.002	0.003	0.004	0.003
8	0.003	0.004	0.005	0.003	0.004
9	0.002	0.003	0.006	0.005	0.002
10	0.002	0.002	0.003	–	–
Average	**0.002**	**0.003**	**0.005**	**0.004**	**0.003**

adversary steals a valid share and tries to spoof the system, the first matching process will be successful. However, the second step will fail due to the *live* facial recognition process. However, if the adversary is able to obtain both a valid share and a photo of the user, the MFA system will be successful. This drawback can be alleviated by movement detection prior to capturing the image, which is a possible direction for future work.

The fact that the proposed work relies entirely on VC and FR for authentication, it is resistant to common attacks such as brute force, dictionary attacks, and hill-climbing attacks. Brute force and dictionary attacks are not applicable as the proposed scheme has no passwords nor secret keys involved. The only option for a brute force attack is to reconstruct the shares of an unknown face image or the face image itself. An attacker would need to guess the N 8-bit pixel values of a share or image, which would result in 2^{8N} possible guesses. Even a small face image with a 128×128 pixel dimension would result in a brute force attack with a complexity of $2^{8\times16384}$ operations, which is still far from feasible based on today's computing capabilities.

A hill-climbing attack is capable of regenerating a face image solely based on match scores provided by the facial recognition algorithm. The general steps involved in a hill-climbing attack are as follows (Adler, 2008):

(1) Choose an initial image estimate and use it as the current image.

(2) Modify the current image based on a random yet biometrically feasible way.

(3) Calculate the match score.

(4) If the match score increases, use the newly modified image as the current image.

(5) Repeat steps 2 to 4 until the match score no longer increases.

As an adversary does not require access to templates, straightforward template encryption via VC does not prevent hill-climbing attacks. Thus, the second authentication factor of the proposed MFA system is susceptible to hill-climbing attacks as it is a direct application of a facial recognition algorithm. However, the overall MFA system is still resistant to hill-climbing attacks due to its first authentication factor, which uses an image share from VC as an authentication token. Image shares produced from VC possess the perfect security property, whereby knowledge of just one share does not provide any information whatsoever of the original secret image (Naor & Shamir, 1995). To impersonate a particular user, an attacker must reconstruct the token for that user. As the tokens are essentially noise, the hill-climbing attack no longer has any advantage over a regular brute force attack.

5.2. Performance

We analyze the performance of the proposed MFA system based on two metrics: efficiency and accuracy. Efficiency is evaluated experimentally by measuring the average time required to authenticate 10 individuals from each database. Based on the results in Table 5, the proposed MFA system requires, on average, 0.03176 seconds to authenticate a user. This depicts the practicality of the proposed method when being used in real-life applications.

Table 6 summarizes the accuracy of the proposed MFA system. We also provide data for the cases whereby BDA was not used to select features for FR. We can clearly see there is an improvement when BDA is used to filter irrelevant features. Each of the authentication factors was first tested individually, then overall MFA system's accuracy was tested by including both authentication factors. We take into account the accuracies when BDA is used for feature selection. Also, to ensure that the experiments reflect upon the practical applications, the FR algorithms are tested using images that were not used for training. Results show that the MFA system can achieve an average recognition rate of 99.81% when tested on all datasets.

Table 5. Average time required to authenticate 10 users.

Databases	Time Required (s)
AR	0.03630
GBU	0.03630
LFW	0.03150
FERET	0.03440
Custom (9 users)	0.02030
Average	**0.03176**

Table 6. Recognition rate (%) comparison.

Databases	1st Factor (No BDA)	1st Factor (With BDA)	2nd Factor (With BDA)	Overall System
AR	97.65	99.96	99.85	99.90
GBU	97.64	99.95	99.88	99.91
LFW	96.40	99.93	99.86	99.89
FERET	96.20	99.90	98.90	99.40
Custom	96.11	99.88	99.98	99.93
Average	**96.80**	**99.92**	**99.69**	**99.81**

6. Conclusion

In this paper, we introduced a user-friendly, privacy-preserving MFA system that can be used in a myriad of practical applications that require non-intrusive authentication such as banking. A novel approach was introduced, whereby the inherent capabilities of facial recognition and visual cryptography were used to formulate an MFA system. Unlike previous MFA systems utilizing VC just for biometric template protection, the proposed MFA approach uses share images produced by VC as authentication tokens. The proposed MFA system is based on two factors, tokens (share images) that are produced by the VC scheme and live face images. Both factors are verified by using the same FR algorithm, thus improving accuracy and reducing implementation cost. To maximize accuracy, we leverage upon BDA to optimize both the VC and FR algorithms in terms of color level and feature selection. As a result, the proposed MFA system was able to achieve a recognition accuracy of up to 99.81%. The main advantages for the proposed system include ease-of-use (users only need to provide their shares to the system), security (the original image encrypted by VC cannot be recovered by using only one of the shares), fast authentication, non-intrusiveness, and near-ideal recognition accuracy. However, it has a complex registration phase, where the training of the FR algorithm is required. For future work, the proposed MFA system can be further accommodated video or 3D images and utilize other biometric modalities such as iris or fingerprints.

Funding

This work is supported in part by the Ministry of Education Malaysia under the Fundamental Research Grant Scheme (FRGS), project number FRGS/1/2019/ICT05/USM/02/1.

ORCID

J. S. Teh http://orcid.org/0000-0001-5571-4148
R. Abdullah http://orcid.org/0000-0002-3061-5837

References

Abhishek, K., Roshan, S., Kumar, P., & Ranjan, R. (2013). A comprehensive study on multifactor authentication schemes. In *Advances in computing and information technology*, Meghanathan N., Nagamalai D., Chaki N. (Eds.), (pp. 561–568). Springer Berlin Heidelberg.

Adler, A. (2008). Biometric system security. In *Handbook of biometrics* Jain, Anil K., Flynn, Patrick, Ross, Arun A (Eds.), (pp. 381–402). Springer US.

Battalglia, F., Iannizzotto, G., & Bello, L. L. (2014). A biometric authentication system based on face recognition and RFID tags. *Mondo Digitale*. http://mondodigitale.aicanet.net/2014-1/augmented_reality_e_biometrics/04_LOBELLO.pdf

Cai, J., Chen, J., & Liang, X. (2015, January). Single-sample face recognition based on intra-class differences in a variation model. *Sensors*, *15*(1), 1071–1087. https://doi.org/10.3390/s150101071

Chengeta, K., & Viriri, S. (2018, March). A survey on facial recognition based on local directional and local binary patterns. In *2018 conference on information communications technology and society (ICTAS)*. IEEE.

European consumers ready to use biometrics for securing payments. (2016). Visa Inc. Retrieved 2020 August, 21, from https://www.visa.co.uk/about-visa/newsroom/press-releases.1478239.html

Hou, Y.-C. (2003, July). Visual cryptography for color images. *Pattern Recognition*, *36*(7), 1619–1629. https://doi.org/10.1016/S0031-3203(02)00258-3

Huang, G. B., Mattar, M., Berg, T., & Learned-Miller, E. (n.d.). *Labeled faces in the wild: A database for studying face recognition in unconstrained environments*. University of Massachusetts. http://vis-www.cs.umass.edu/lfw/

Ibrahim, D. R., Abdullah, R., Teh, J. S., & Alsalibi, B. (2019). Authentication for ID cards based on colour visual cryptography and facial recognition. In *Proceedings of the 3rd international conference on cryptography, security and privacy - ICCSP '19*. Kuala Lumpur, Malaysia: ACM Press.

Ibrahim, D. R., Tamimi, A. A., & Abdalla, A. M. (2017, May). Performance analysis of biometric recognition modalities. In *2017 8th international conference on information technology (ICIT)*. IEEE.

Judith, I. D., Mary, G. J. J., & Susanna, M. M. (2016, February). Three factor biometric authentication for spiraling of security. In *2016 international conference on emerging trends in engineering, technology and science (ICETETS)*. IEEE.

Kumar, M., Jindal, M. K., & Sharma, R. K. (2011, November). k-nearest neighbor based offline handwritten gurmukhi character recognition. In *2011 international conference on image information processing*. IEEE.

Lin, W.-H., Wu, B.-H., & Huang, Q.-H. (2018, April). A face-recognition approach based on secret sharing for user authentication in public-transportation security. In *2018 IEEE international conference on applied system invention (ICASI)*. IEEE.

Martinez, A. M., & Benavente, R. (n.d.). *The AR face database*. Ohio State University. http://www2.ece.ohio-state.edu/˜aleix/ARdatabase.html.

Mirjalili, S. (2015, May). Dragonfly algorithm: A new meta-heuristic optimization technique for solving single-objective, discrete, and multi-objective problems. *Neural Computing & Applications*, *27*(4), 1053–1073. https://doi.org/10.1007/s00521-015-1920-1

Mohammed, A. J., & Yassin, A. A. (2019, September). Efficient and flexible multi-factor authentication protocol based on fuzzy extractor of administrator's fingerprint and smart mobile device. *Cryptography*, *3*(3), 24. https://doi.org/10.3390/cryptography3030024

Mwema, J., Kimwele, M., & Kimani, S. (2015, February). A simple review of biometric template protection schemes used in preventing adversary attacks on biometric fingerprint templates. *International Journal of Computer Trends and Technology*, *20*(1), 12–18. https://doi.org/10.14445/22312803/IJCTT-V20P103

Nanni, L., Brahnam, S., & Lumini, A. (2012, October). A simple method for improving local binary patterns by considering non-uniform patterns. *Pattern Recognition*, *45*(10), 3844–3852. https://doi.org/10.1016/j.patcog.2012.04.007

Nanni, L., & Lumini, A. (2008, November). Local binary patterns for a hybrid fingerprint matcher. *Pattern Recognition*, *41*(11), 3461–3466. https://doi.org/10.1016/j.patcog.2008.05.013

Naor, M., & Shamir, A. (1995). Visual cryptography. In *Advances in cryptology — EUROCRYPT'94*, Alfredo De Santis (Ed.), (pp. 1–12). Springer Berlin Heidelberg.

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018, January). Multi-factor authentication: A survey. *Cryptography*, *2*(1), 1. https://doi.org/10.3390/cryptography2010001

Phillips, P., Moon, H., Rizvi, S., & Rauss, P. (2000). The FERET evaluation methodology for face-recognition algorithms. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *22*(10), 1090–1104. https://doi.org/10.1109/34.879790

Phillips, P. J., Beveridge, J. R., Draper, B. A., Givens, G., O'Toole, A. J., Bolme, D., Dunlop, J., Lui, Y. M., Sahibzada, H., & Weimer, S. (2012, March). The good, the bad, and the ugly face challenge problem. *Image and Vision Computing*, *30*(3), 177–185. https://doi.org/10.1016/j.imavis.2012.01.004

Sakaue, F., & Shakunaga, T. (2005). Combination of projectional and locational decompositions for robust face recognition. In *Lecture notes in computer science,* Zhao W., Gong S., Tang X (Eds.), (pp. 407–421). Springer Berlin Heidelberg.

Sakaue, F., & Shakunaga, T. (2006). Gaussian decomposition for robust face recognition. In *Computer vision – ACCV 2006,* Narayanan P.J., Nayar S.K., Shum HY (Eds.), (pp. 110–119). Springer Berlin Heidelberg.

Sandhya, M., & Prasad, M. V. N. K. (2016, December). Biometric template protection: A systematic literature review of approaches and modalities. In *Signal processing for security technologies,* Jiang R., Al-maadeed S., Bouridane A., Crookes P., Beghdadi A (Eds.), (pp. 323–370). Springer International Publishing.

Sangaiah, A. K., Hosseinabadi, A. A. R., Shareh, M. B., Rad, S. Y. B., Zolfagharian, A., & Chilamkurti, N. (2020, January). IoT resource allocation and optimization based on heuristic algorithm. *Sensors*, *20*(2), 539. https://doi.org/10.3390/s20020539

Sangaiah, A. K., Medhane, D. V., Bian, G.-B., Ghoneim, A., Alrashoud, M., & Hossain, M. S. (2020, May). Energy-aware green adversary model for cyber-physical security in industrial system. *IEEE Transactions on Industrial Informatics*, *16*(5), 3322–3329. https://doi.org/10.1109/TII.2019.2953289

Sangaiah, A. K., Medhane, D. V., Han, T., Hossain, M. S., & Muhammad, G. (2019, July). Enforcing position-based confidentiality with machine learning paradigm through mobile edge computing in real-time industrial informatics. *IEEE Transactions on Industrial Informatics*, *15*(7), 4189–4196. https://doi.org/10.1109/TII.2019.2898174

Singh, G., & Chhabra, I. (2018). Genetic algorithm implementation to optimize the hybridization of feature extraction and metaheuristic classifiers. In *Hybrid metaheuristics for image analysis,* Bhattacharyya S. (Ed.), (pp. 49–86). Springer International Publishing.

Steam Guard Mobile Authenticator. (2017). Valve Corporation. Retrieved 2020 August 21, from https://support .steampowered.com/kb article.php?ref=8625-WRAH–9030

Suryadevara, S., Naaz, R., Kapoor, S., & Sharma, A. (2011, September). Visual cryptography improvises the security of tongue as a biometric in banking system. In *2011 2nd international conference on computer and communication technology (ICCCT-2011)*. IEEE.

Venukumar, V., & Pathari, V. (2016, September). Multi-factor authentication using threshold cryptography. In *2016 international conference on advances in computing, communications and informatics (ICACCI)*. Jaipur, India: IEEE.

Vinay, A., Shekhar, V. S., Manjunath, N., Murthy, K. N. B., & Natarajan, S. (2017, September). Expediting automated face recognition using the novel ORB2-IPR framework. In *Proceedings of international conference on cognition and recognition,* D. S. Guru, T. Vasudev, H.K. Chethan, Y.H. Sharath Kumar (Eds.), (pp. 223–232). Springer.