

Visual Cryptography based Authentication of Fog Devices

Mradula Sharma and Parmeet Kaur

Department of Computer Science & Engineering and Information Technology,
Jaypee Institute of Information Technology, Noida, India

E-mail: mradula.sharma@jiit.ac.in, parmeet.kaur@jiit.ac.in

(Received April 26, 2023, Accepted June 10, 2023)

Abstract: Visual cryptography (VC) is a method of distributing secret images in the form of shares to different users. Each share displays either random noise or a random binary pattern. A secret image is visible only when all shares are stacked together. The paper proposes a cloud-fog architecture in which the cloud server uses VC technique to authenticate the Fog devices trying to connect with it. A secret code is generated by the cloud server and divided into two shares, one of which is shared with the fog device. When a fog device connects to a cloud server, it sends the shared image to the cloud. The cloud then stacks the received share image with its own share image. If the secret image is shown, the fog device is verified and can transfer data or communicate with the cloud server. Further, the proposed architecture uses K out of N visual cryptography to authenticate the group of Fog devices, where K shares out of N are required to reveal the secret image.

Keywords: Visual cryptography, Fog computing, Secret sharing, Image processing.

1. Introduction

Fog computing is a distributed computing paradigm which provides compute and storage resources in proximity to the data source. Fog nodes support the cloud services by reducing the latency of time-critical applications as well as the bandwidth required for communication with the cloud. Since front-end fog nodes provide services to numerous end users and generally handle user data, authentication of these nodes is a critical issue to prevent any privacy or security breaches in the fog-cloud environment. Numerous fog devices can connect to the cloud and send data. Authentication of the fog devices is required before setting up a communication link for data transmission and subsequently, receipt of results. The process of identifying a device is called authentication while granting permissions is called

authorization. Only approved devices are able to connect with cloud accounts, gateways, and other devices. System administrators register devices before adding them. The system examines all linked devices as well as gadgets that exchange data with one another. Public key infrastructures (PKIs) are used by many businesses to link device IDs with certificates of authenticity provided by trusted third-party certificate authorities¹. PKI solutions are the responsibility of a third-party provider and require high bandwidth and processing power. Hence, there is a need for low-overhead methods for authentication of fog devices.

The existing authentication methods vary depending on the location of the device and the type of data the device is sending or receiving. These lie in the categories of either centralized or decentralized security models. In the distributed models, the device itself is responsible for storing identities, confirming authorization, and creating certificates. In contrast, in a centralized model, the management and distribution of fog device authentication is handled by a central server or application managed by a trusted third party. When the device connects to the network, the central certificate store performs the connection verification and authentication processes.

In addition, there are two methods for distributing authentication: single-way authentication and mutual authentication, sometimes known as two-way authentication². It is referred to as distributed one-way authentication when two devices, such as a fog device and a cloud server, connect to each other and only one of the devices authenticates with the other device while the other device does not authenticate itself. Using a password hash or digital certificates, the first device verifies itself as legitimate with the second device. The second device verifies the password or certificate and compares it to the stored data when the first device makes an attempt to connect. The device approves the creation of the connection if the data is accurate.

In comparison, mutual verification is an additional authentication method in which both devices verify each other's identities before communicating. Before the identities can be compared, each device must store a unique digital identification for the other device. An administrator registers the devices with a central authority or server and issues genuine digital certificates as part of centralised authentication. A secure handshake between two communication devices is made simpler by the centralised authority. In this category, security certificates are not saved on the device, preventing theft. The devices still have strong security, though. Some authentication-based protocols have been used to authenticate the fog node. The message queuing telemetry transport (MQTT) protocol is used to connect a client, such as an Internet of Things

device, to a broker³. The broker holds digital identities and certificates. IT workers may use MQTT in network monitoring and management solutions to keep track of thousands of IoT devices. For the Secure Mutual Authentication Protocol for Fog/Edge (SMAP)⁴ procedure to begin, there must be at least two communicating parties that desire to establish secure connection as well as an authentication server AS. This protocol maintains secrecy with public key encryption, integrity with one-way hashing, and mutual agreement between communicating parties decides the final session key for authentication in the case of communication. The authentication server AS maintains all public keys.

In this research, we suggested a cloud-fog architecture in which the cloud server uses visual cryptography to verify the authenticity of the Fog devices trying to connect to it. The cloud provides resources at a large scale and does not need to be authenticated by each fog node. However, fog nodes are dynamically added and removed from the system and may be compromised. Hence, we propose a one-way authentication for verifying the identity of fog nodes. We assume that the fog devices authenticate the IoT devices that connect to them. Following data aggregation and analysis, fog nodes are required to connect to a cloud server. To authenticate the fog nodes, visual cryptography is used and an architecture is proposed for the same. Using the VC technique, the cloud server generates a secret code and divides it into two shares, one of which is shared with the fog device with which the cloud server will need to communicate with later. When a fog device connects to a cloud server, the shared image is transmitted to the cloud. The cloud then stacks the received share image on top of its own. If the secret image is displayed, the fog device has been validated and is ready to transfer data or communicate with the cloud server.

The rest of the paper is organized as follows: Section II reviews the literature and describes visual cryptography; Section III describes the fog-cloud architecture and proposed authentication technique. An analysis of our approach with experimental results is discussed in Section IV. In the end, we draw a conclusion and outline the extent of the work that remains.

2. Literature Survey

Shamir⁵ first came up with the idea of using visual cryptography as a secret sharing method in 1996. Decryption uses the human visual system, making this particular cryptographic method one that does not require a cryptographic computational method. restore hidden image. Using this method, a message is delivered to many different users in the form of shares.

Each share has nothing but a random bit pattern. When all shared shares are collected and stacked on top of each other, the message can become visible. However, we are unable to obtain information from individual share. The parameters of visual cryptography are as follows: the first is called contrast and the second is called single-pixel dilation. The contrast, sometimes referred to as the relative difference, is the distinction between the stacked subpixels that form a white or black pixel. The pixel pitch is the quantity of subpixels needed to encode a black or white pixel. During pixel dilation, each hidden pixel is coded into subpixels when divided, making the divisions many times larger than the hidden image. To get the best results, we need pixel dilation as minimal as possible while maximising relative difference, or contrast.

Visual cryptography, originally proposed by Noar and Shamir, involves sharing a secret image across multiple shares. Shamir⁵ presented a K-out-of-N visual cryptographic secret-sharing scheme for black-and-white images. The dealer encrypts the secret for each of the N participants, and the shared secret (which could be printed text, handwritten notes, images, etc.) can be revealed without cryptographic computations. In a K-out-of-N visual cryptographic scheme, the dealer divides the secret into N transparent shares, distributing one to each participant. When at least K participants align their shares, the secret is revealed. However, when fewer than K shares are overlaid, the secret remains hidden. Visual cryptography offers a wide range of applications, such as copyright protection⁶, access control⁷, watermarking⁸, and authentication⁹. It enables the secure embedding of copyright information in images to verify digital asset authenticity and ownership. Additionally, it facilitates access restriction to sensitive data by mandating multiple parties to present their shares for secret revelation. Visual cryptography can also be employed to embed undetectable watermarks in digital media, deterring unauthorized users from removing or altering them. Moreover, it plays a crucial role in authentication systems by confirming the identity of users or devices through the presentation of specific shares to gain system access. Overall, visual cryptography is a unique and powerful method for sharing and protecting confidential information. Its reliance on the human visual system for decryption makes it an attractive solution for various applications, including those involving low-power devices or environments where computational resources are limited.

In a secret binary image, each pixel is encoded as a pair of black-and-white subpixels distributed across two shares, as illustrated in Figure 1. When a pixel in Figure 1 is either white or black, one of the two possible white/black combinations listed below the pixel is selected, with each row having a 50%

chance of being chosen randomly. The subpixels in the Share 1 column are assigned to the first share, and the subpixels in the Share 2 column are allocated to the second share. Regardless of whether the pixel is black or white, it is divided into two subpixels with an equal probability of black-white or white-black pairings. Consequently, a single share cannot differentiate between black and white pixels.

Original Pixel	Share 1	Share 2	Stacked Share
			
			
			
			

Figure 1: Two-out-of-two Visual Cryptography Scheme⁵

Consider the two shares that are stacked as seen in the last column of Figure 1. When two shares overlap, two additional black pixels are created if a pixel is completely black. On the other hand, if the pixel is white, it produces a subpixel that is half-black and half-white, resulting in one white pixel and one black pixel (medium grey). By stacking the two shares, it is possible to get all of the information from the hidden image.

A lot of research is done on visual encryption for binary images. The researchers¹⁰⁻¹¹ expanded visual cryptography to grayscale images. The authors¹⁰ studies generic access VC for pictures with m grey levels from 0 to $m-1$. Instead of capturing grey levels or grey subpixels, the authors¹¹ recommended utilising VC for grey level pictures using dithering methods. This is in place of taking grey levels. Using dithering¹¹, a greyscale picture is converted into something like a binary image, and then shares are created using current visual cryptography. The author¹² devised a grey level visual cryptography technique by transforming a grey level picture to a halftone image and then used a simple binary visual cryptography scheme. The work¹² also proposed visual cryptography systems for colour pictures. In these schemes, images are first colour-decomposed to separate them into three channels (yellow, magenta, and cyan), and then they are half-toned. This is completed before visual cryptography is used to encrypt shares.

3. Proposed Authentication Method

IoT devices and sensors produce enormous amounts of data, but they are unable to process it locally due to memory and CPU limitations. In order to process data, it must be uploaded to the cloud. IoT devices need high-speed internet to send data to the cloud for processing and to return information to consumers. The use of fog-based processing improves processing efficiency and reduces latency. It is predicated on the notion that all data that is created must be processed on fog devices that are situated inside a local area network (LAN). LAN-based fog machines analyse massive volumes of fresh data and periodically send a summary to the cloud. As a result, fog-based devices serve as a bridge between the devices that comprise the Internet of Things and the cloud¹³. The cloud must authenticate the fog nodes before connecting them to the cloud servers. Therefore, we use the architecture of Figure 2 and propose to authenticate the fog nodes using visual cryptography technique⁵.

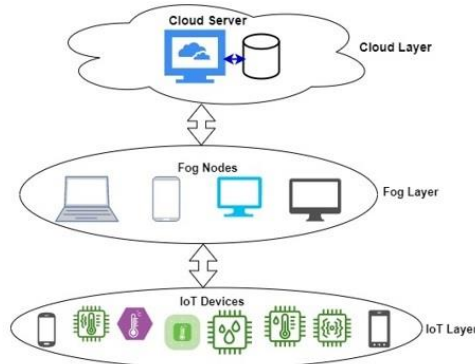


Figure 2: Cloud-Fog-IoT Layer architecture

Visual cryptography is a method that enables the encryption of an image into multiple shares while ensuring that each share conceals all traces of the original image. Without any computational decryption, the original image can be visually recreated when the necessary number of shares are combined. Place share1 and share2 on top of one another as in Figure 1 to reveal the original image. This is because when a white pixel is combined with its inverse, it will result in a white pixel, while combining two black pixels will result in a black pixel. In a basic two-out-of-two VC scheme, each input image pixel is expanded into a 2x2 block of pixels in the generated shares. As a result, the shares would be larger while maintaining the same aspect ratio as the original image (e.g., twice the width and height of the input image). This pixel expansion may result in a reconstructed image that appears larger and potentially less visually appealing than the original image. In order to

maintain the aspect ratio and size of the original image in the shares, we utilized an extended VC method as proposed¹⁴. This method ensures that the generated shares have the same aspect ratio and dimensions as the original image, resulting in a reconstructed image with enhanced visual quality and clarity.

Proposed Algorithm 1

1. Let F be the set of fog devices and C be the cloud server
2. For each fog device f_i in F that needs to communicate with C :
 - 2.1 Generate a unique secret code S_i
 - 2.2 Divide S_i into two shares: $share1_i$ and $share2_i$, such that $S_i = share1_i \oplus share2_i$
 - 2.3 Store $share1_i$ in cloud storage
 - 2.4 Transfer $share2_i$ to the corresponding fog device f_i
3. When a fog device f_i requests access to the cloud storage:
 - 3.1 Fog device f_i sends $share2_i$ to C
 - 3.2 Cloud server C retrieves $share1_i$ from cloud storage
 - 3.3 Calculate the resultant share R_i as $R_i = share1_i \oplus share2_i$
 - 3.4 Compare R_i with the original secret code S_i
 - 3.5 If R_i equals S_i :
 - 3.5.1 Authenticate the fog device f_i
 - 3.5.2 Grant access to cloud storage for f_i
 - 3.6 Else:
 - 3.6.1 Do not authenticate the fog device f_i
 - 3.6.2 Deny access to cloud storage for f_i

In the proposed authentication method, as shown in Figure 3, cloud will generate a unique secret code for each fog device it needs to communicate with. The cloud server divides the code into two shares, for example share1 and share 2. The share 1 is stored in cloud storage and share 2 is transferred to the fog device. Whenever fog device wishes to connect to the cloud, it has to send share 2 to the cloud before accessing the cloud storage.

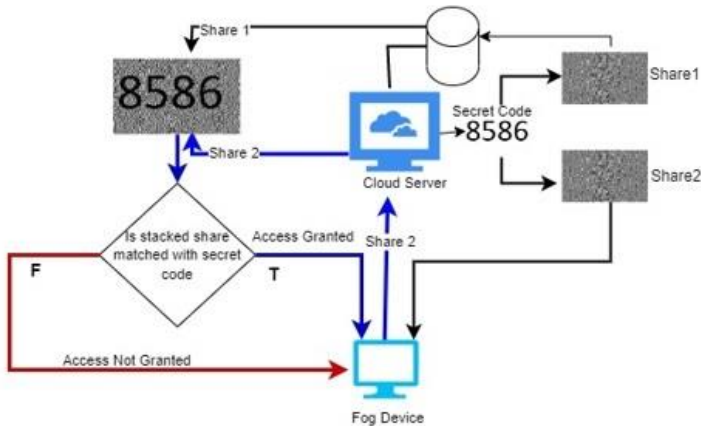


Figure 3: Proposed architecture to authenticate the fog device using VC technique

Now, cloud will stack the share 2 with share 1 and get the resultant share. If resultant share is matched with the secret code, the fog device is authenticated and granted the access of cloud storage. If resultant share does not match then fog device is not authenticated and not provided access to the cloud storage. The working of this proposed method is described in Algorithm1. To authenticate the group of fog devices, the proposed method will use the K out of N visual cryptography. A secret code is encoded and divided into N different share. Each share shows nothing more than a binary random pattern. At least K (threshold) of N shares must be acquired collectively to disclose the secret code. Even with infinite computing power, the secret code can't be found unless at least k share images are put together.

4. Results

The outcomes of the suggested authentication mechanism for fog devices are shown in this section. MATLAB was used to implement the simulations. We have used a number of colour and grey level test photos as secret codes. These are illustrated in Figure 4. It is assumed that the cloud server generates these secret codes. The secret information is encoded in the form of shares.



Figure 4: Secret codes



a. Secret Text b. cloud Share1 c. fog device Share 2 d. Overlapped b & c

Figure 5: Two out of two Visual cryptography (Binary Image)

A random number of pixels in black and white are included in each share. In the case of N out of N visual cryptography, it is impossible for anyone to decipher the secret code by using a single share unless and until all of the shares are stacked together. In K out of N visual cryptography, at least K shares must be joined in order to extract the secret code. The secret code cannot be

revealed by any $K-1$ shares. A cloud server has the ability to simultaneously authenticate $K-1$ fog devices. The implementation of both types of visual cryptography is depicted in Figures 5 to 7. In the two-out of-twoVC technique, as depicted in Figure 5, one share is held by the cloud and the other is sent to the fog device. To authenticate the fog device, cloud share and share of fog device are brought together to reveal the secret code. The fog device is verified if the secret code matches the cloud-generated code. Figure 6 illustrates the implementation of the K out of N Visual Cryptography technique when more than one fog device wants to be authenticated by the cloud. In Figure 7, K is three and N is four, so $K-1$ shares of fog devices and cloud shares are stacked to reveal the secret code. $K-1$ fog devices are authenticated if the code matches the generated secret code.

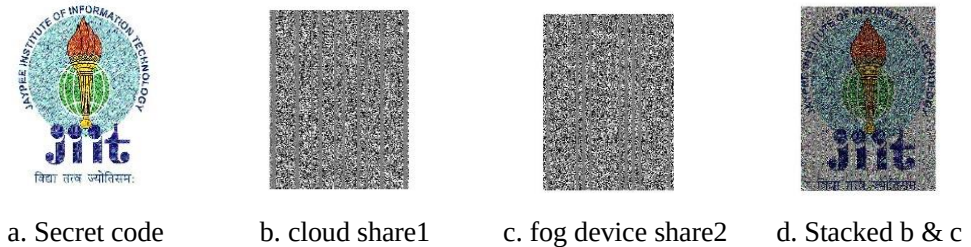


Figure 6: Two out of two Visual cryptography (Colour Image)

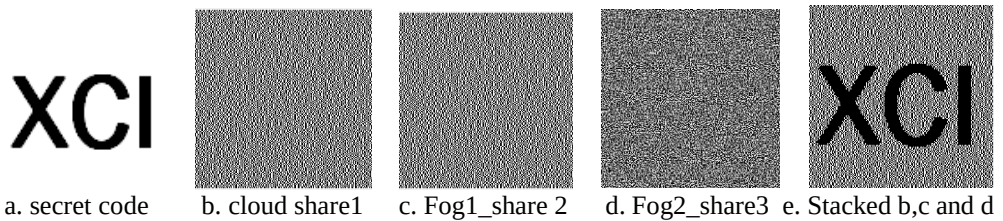


Figure 7: Three out of four visual cryptography

4. Conclusion & Future Work

The paper has proposed a cloud- fog architecture where fog devices are authenticated using visual cryptography method. It is a light weight method for one-way authentication that does not impose any high overhead on the fog device. The working of the proposed method has been verified using sample codes. In future, the work can be extended to enhance the security of the share itself during transmission between cloud and fog devices using encryption. This will prevent tampering of the shares in visual cryptography. This work can also be extended to create pixel expansion-free meaningful shares.

References

1. Kim, Hokeun, and Edward A. Lee; Authentication and Authorization for the Internet of Things, *IT Professional* 19(5) (2017), 27-33.
2. Woo, Y C Thomas and Simon S. Lam; Authentication for distributed systems, *Computer* 25(1) (1992), 39-52.
3. Hunkeler, Urs, Hong Linh Truong and Andy Stanford-Clark; MQTT-S- A publish/subscribe protocol for Wireless Sensor Networks, *3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE'08)*, IEEE, (2008), 791-798.
4. M. S. Pardeshi and S. -M. Yuan; SMAP Fog/Edge: A Secure Mutual Authentication Protocol for Fog/Edge, *IEEE Access*, 7 (2019), 101327-101335.
5. Naor, Moni, and Adi Shamir; Visual cryptography, In *Workshop on the Theory and Application of Cryptographic Techniques*, Springer, Berlin, Heidelberg, (1994), 1-12.
6. Lou, Der-Chyuan, Hao-Kuan Tso and Jiang-Lung Liu; A copyright protection scheme for digital images using visual cryptography technique, *Computer Standards & Interfaces*, 29(1) (2007), 125-131.
7. Chen, Yi-Hui, Chi-Shiang Chan, Po-Yu Hsu and Wei-Lin Huang, Tagged visual cryptography with access control, *IEEE International Conference on Multimedia and Expo Workshops (ICMEW)*, (2014), 1-5.
8. Stelvio Cimato, James CN Yang and Chih-Cheng Wu, Visual cryptography based watermarking, *Transactions on Data Hiding and Multimedia Security IX: Special Issue on Visual Cryptography* (2014), 91-109.
9. Sain, Kunal, Mradula Sharma and Suneeta Agarwal; ASPS: an authentication scheme using pre-formed visual cryptographic shares, *Proceedings of the Fifth International Conference on Security of Information and Networks*, (2012), 183-187.
10. C. Blundo, A. D. Santis and M. Naor; Visual cryptography for grey level images, *Information Processing Letters*, 75(6) (2000), 255-259.
11. C.-C. Lin and W.-H. Tsai; Visual cryptography for gray-level images by dithering techniques, *Pattern Recognition Letters*, 24(13) (2003), 349-358.
12. Y.-C. Hou; Visual cryptography for color images, *Pattern Recognition*, 36(7) (2003), 1619-1629.
13. Stojmenovic, Ivan, Sheng Wen, Xinyi Huang and Hao Luan; An overview of fog computing and its security issues, *Concurrency and Computation: Practice and Experience*, 28(10) (2016), 2991-3005.
14. Mradula Sharma, Kunal Sain and Suneeta Agarwal; GES: A Group based Encoding of Shares for Visual Cryptography without Pixel Expansion, *International Journal of Computer Applications* 975 (2014), 8887.