



Implementation of STAGO-VCs to Secure the Food Grain Distribution System

Manish Prajapati¹, Suresh Prasad Kannoja^{2*}

¹ M.Sc.(cs) Student, ²Assistant Professor

^{1,2}Department of Computer Science

^{1,2} University of Lucknow, Lucknow, India

*Corresponding Author: spkannoja@gmail.com, Mobile: +91-8840880224

Abstract: Visual Cryptography is one of the technics to convert secret information into an unreadable format and is used to break private visual data into numbers of shares and is easily maintainable at different locations. However, any person never accesses the original data unless all shares are available. The main objective of this paper is to ensure control of bogus ration cards, minimize the leakage of food grains and avail flexible and secure rationing systems. In this paper, a new Smart Ration Card technique has been proposed, which is based on a dual authentication mechanism that also fulfils the security of biometric data and maintains individual information.

Index Terms - Visual Cryptography, Steganography, Secure, Biometric Security.

I. INTRODUCTION

The public distribution system (PDS) is an Indian Food Security system. This was established by the Government of India under the Ministry of Consumer Affairs, Food, and Public Distribution to distribute food and non-food items to India's poor people at subsidized rates. India has the largest stock of food grains in the world after China, India government spends about Rs.750 billion. The distribution of food grains to poor people throughout the country is managed by state governments as per the report of 2011, there were 505,879 fair price shops (FPS) across India. The ration card is an official document issued by the government of India to obtain subsidized food grains from the fair price shops run by the Food Corporation of India through the network of the Public Distribution System. The performance of any system depends on the policies and security mechanisms and way of implementation to run the system properly, the People have lots of challenges in the public distribution system, unavailability of flexible and secure rationing is one of them. In the Traditional Ration Card System, one ration card booklet is provided to each family. Anyone can take the food grains through your ration card easily because in TRDS no technique has been used for user authentication during the ration distribution. Therefore, it is an unsecured system because if a ration card is lost and anyone can find it other than our family member and get the ration of estimated quota that is not fair for families dependent on that ration. The people need a dual secure distribution system.

So here we are introducing a new and efficient ration card system based on a biometric fingerprinting system to authenticate family members. Using this we can reduce ration theft. The system operates by getting raw biometric data from a subject and then extracting the feature set from the objects and comparing that feature set with the template stored in a database, the template of a person in the database is generated during enrolment and is often kept with original raw data. Further, during the registration process, the original template of biometric data is stored in any third-party storage or database and is well-secured by external threats and attackers, but we can't guarantee internal threats. An authorized person easily accesses individual biometric data and can unwantedly use it anywhere. It is necessary to store these data in some encrypted format if any unauthorized person wants to access it, and can't use that data without our permission.

This paper is organized into five sections: Section I Provides the introduction to the existing public distribution system, the traditional ration card system, and the need for an efficient card system. Section II contains the related work of steganography, biometric data, various security mechanisms, and visual cryptography. Section III included the proposed model based on the dual authentication process, experimental setup, security, and share generation algorithms. Section IV discusses the result & analysis, and the conclusion and future scope are provided in Section V.

II. RELATED WORK

Visual Cryptography for Biometric Privacy Arun Ross, Senior Member, IEEE, and Asem Othman, talk about the protection of various biometric data like iris, fingerprint, and face images through visual cryptography techniques.

Shawn D. Dickman, in "An Overview of Steganography" gives a brief overview of the steganography scheme, how it works, what is a historical example of steganography, what steganography software is commercially available, and what data types are supported, etc. he also analyses challenges faced in steganography while transmitting our data.

Bhakta, Anupam, et al. state a new approach to hiding a secret image through a visual cryptography scheme. In this scheme he uses a variable length image key to encrypt the original image then the bit sieve procedure is used on the resultant image and lastly, they perform a K-N secret sharing scheme on the final encrypted image. Decryption is done in the reverse level of encryption, bit sieve method, and image key decryption respectively.

Aarti, Pushpendra K Rajput, "An EVCS for Color Images with Real Size Image Recovery and Ideal Contrast Using Bit Plane Encoding" Provides a new way of sharing generation in extended visual cryptography techniques using bit-plane encoding. He also generates a meaningful share that is easily recognizable and managed.

S. P. Kannoja, Jasvant kumar, "Secure Rationing System through Visual Cryptography: Smart Ration Card" Provides a mechanism to build an improved and secured ration card system to control bogus ration cards and leakage of food grains, only limited to binary images.

C Prabhu, Nivedha, et.al, "Multiple Image Steganography using LSB-DCT Technique" provide the LSB-DCT technique to hide multiple images in one cover image.

III. METHODOLOGY

Proposed Model:

A new efficient Smart ration card system based on facial images and biometrics that can reduce leakage of food grain and theft, to avoid corruption in the food grain distribution system has been proposed.

The proposed model is based on the biometric authentication system in which individual identity has been checked, whether it is a family member or not. The basic design of the proposed Smart ration card is shown in fig.1.

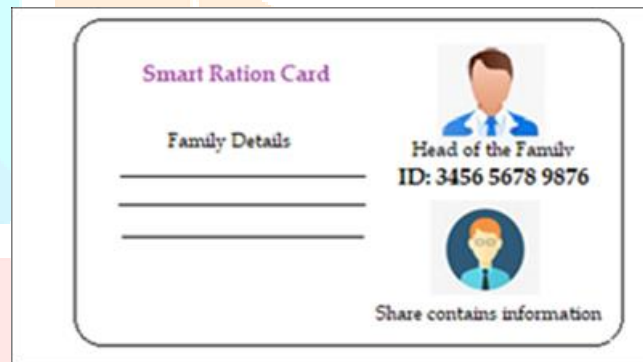


Fig. 1. Smart ration card for secure food grains distribution system.

The fingerprint information of family member has stored in the database in an encrypted format and accessed through this provided card. The individual who brings the card to take rations gives his fingerprint information, and after that match is performed with stored family biometric data, if his fingerprint is matched with any one of the members then he can easily purchase the rations otherwise unable to purchase grain from the system.

The main characteristics of the proposed model are a dual authentication system and two-level of data security.

Dual Authentication mechanism: The first authentication performs by checking the card personnel who have this card and can allow purchasing food grains. This is necessary because the card has a unique ID number that provides each family information (like how many family members are, the amount of rations quantity allotted in their quota, etc.) and access to their biometric database. This card also contains one part of encrypted share information in the head of the family image or other image.

Two-level security of data: This Ration card is implemented through two levels of security mechanism. By which family privacy maintains and avoids the unwanted use of biometric data. These data are stored in encrypted format in multiple shares, one part of the shares is stored in the database and the other part of the share is provided on a ration card that is kept by a family member. Whenever any person come for purchasing a ration then the first level of security checks the basic detail of a person using the smart ration card if a person is verified then in the second level the biometric operation is performed. If a person's biometric information is matched with family member data, then he is said to be a valid member of the family and allow to buy a ration.

The whole process of the proposed model is divided into two Phases.

Phase 1: Enrolment phase

Phase 2: Authentication phase

A. Phase 1 Enrolment phase: This phase consists of two parts.

Part 1: The biometric data of the whole family member is taken. Then data is sent to a trusted third-party entity. Once the trusted entity receives it, the encryption of data is performed as encryption all biometric data is combined and then this

combined data is hidden using the proper steganography technique (i.e. LSB insertion technique) in the cover image. Here we are taking the image of the head of a family as a cover image using Algo1.

Part 2: Generated stego image provided as input in XOR-based visual cryptography algorithm, two encrypted share is generated and covered with the family head image. One part of generated share is stored in a database that manages ration card details and another part of this is stored in a ration card which is available to the family using Algo2.

Algorithms used in Phase 1

Algo 1: Algorithm used to insert data image into the cover image:

Input: Cover Image, all member fingerprint data

Output: Stego Image containing hidden data

Begin

Step 1: Read the cover image.

Step 2: Bit slice cover image to Red, Green, and Blue Planes.

Step 3: Read all fingerprint images to be hidden. Combine all biometric images into one container image.

Step 4: Select the container image and convert it into binary bits

Step 5: Now replace bits of the Cover image in order of 3:3:3 of the LSB in three planes (i.e. Red, Green, and Blue planes) with the bits of the container image.

End

Algo 2: Algorithm used to convert stego image into encrypted share

Input: Stego Image, shares size ($s_size = 2$)

Output: Two encrypted share

Begin

Step1: Take an image as input and convert it into array format.

Step2: Now calculate the width, height, and depth of an array

Step3: Generate a shared array of random values 0 to 255 with the same size as an image, shares array divided in bit plane of s_size .

Step 4: Binary pixel value of original image stored into a shares array as

Shares $[:, :, :-1] = \text{image. copy}()$

Step 5: Now bit sieved operation is performed by combining the bit planes of the original image, which will be combined with the bit planes of the Key image randomly using the XOR operation.

for $i = 0$ to s_size

```
{
shares[:, :, -1] = shares[:, :, -1] [xor] shares[:, :, i]
}
```

Step 6: Generated bit-sieved array containing both shares is extracted and saved in the form of an image.

End

The Two-level security implementation through steganography and visual cryptography approach are shown in fig.2

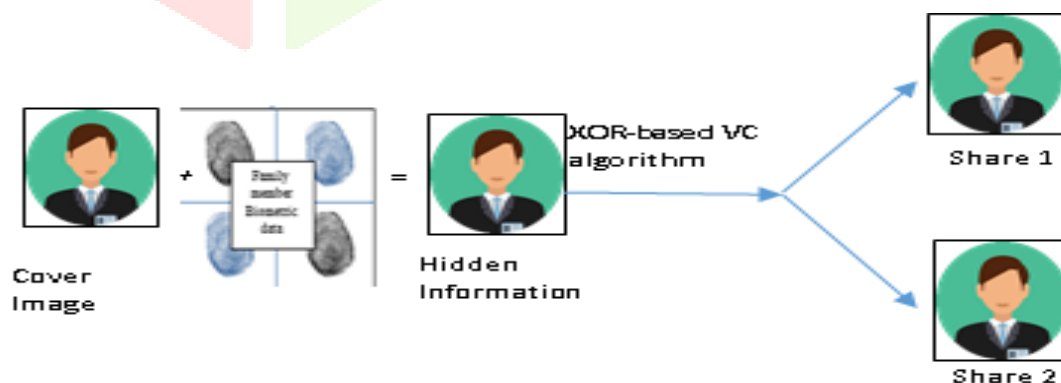


Fig. 2. Shows the Two-level security implementation through steganography and visual cryptography approach

Fig. 3.

B. Phase 2: Authentication phase

The authentication phase starts when any member of the family or someone else brings a ration card to purchase a ration at the shop. He provides one part of the share that is available on the card and the unique id number by which the stored share from the database is accessed, stacking is performed, and biometrics of all family members are accessed after that match is performed on a person's biometric data. The complete authentication process is shown in fig3.

Algorithms used in Phase 2

Algo 3: Algorithm used to decrypt two encrypted shares

Input: Two shares S1 and S2

Output: A Stego image containing hidden data

Begin

Step 1: The receiver reads the encrypted data

Step2: S1 and S2 are converted into an array then a bitwise XOR operation is performed and the result is stored in a new array.

Step 3. The generated array is now converted into an unsigned integer and then saved in the form of an image.

End

Algo 4: Algorithm used to retain data image from the Stego image:

Input: Stego image

Output: Secret biometric data of each member

Begin

Step 1: Load the reconstructed image from the stored location.

Step 2: Separate bits of the message image in order of 3:3:3 of the LSB in three planes (i.e. Red, Green, and Blue planes) from the image with a hidden message.

Step 3: De-interleave and arrange the bits to reconstruct the message images.

Step 4: A container image is obtained after the Edge Tapering process.

Step 5: Separate each biometric data from its content and store it in the proper place

End

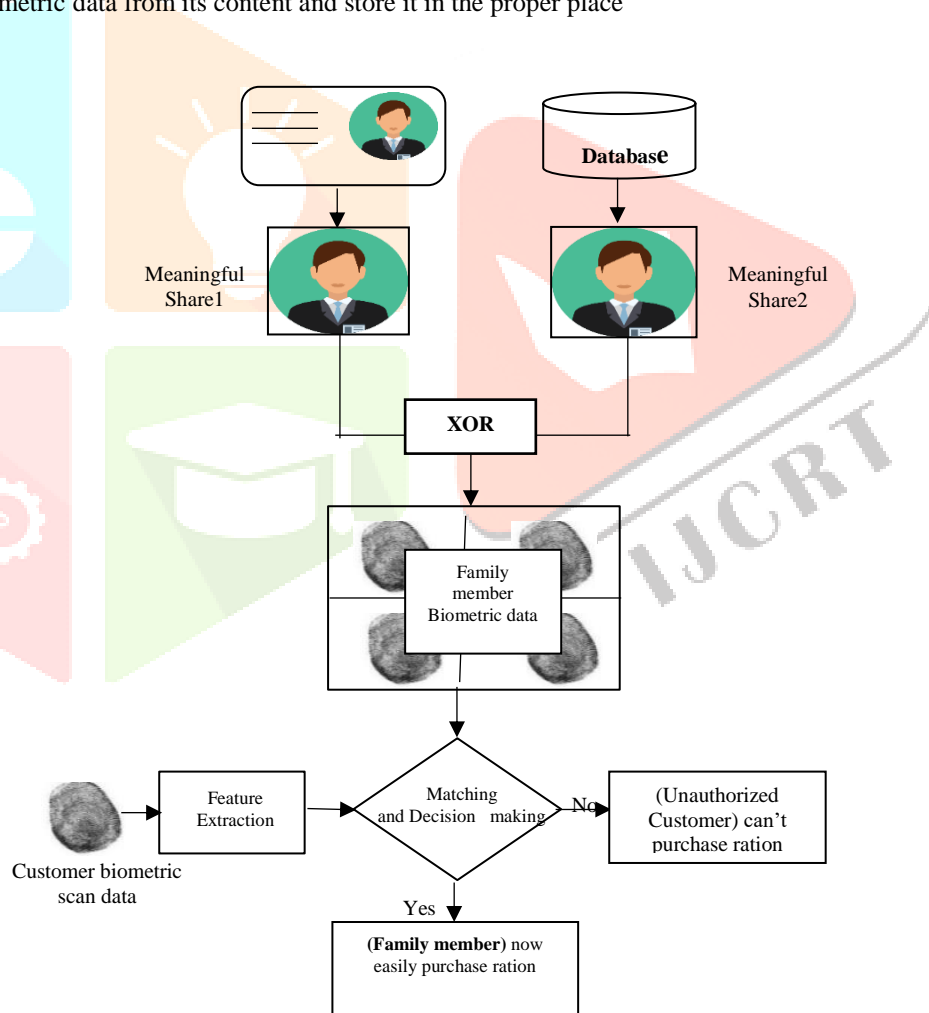


Fig. 4. Shows the share authentication process

C. Experimental Setup: It consists of three steps

Step 1: Python Installation

The experimental setup has been performed on a Dell Vostro tower model Machine having Intel(R) Core (TM) i5-7400 CPU @ 3.00GHz 3.00 GHz, windows 10 pro, with Installing Python, Verify Pip was installed using pip -V command: Pip is a powerful package management system for Python.

Step 2: PyCharm installation

PyCharm is a dedicated Python Integrated Development Environment (IDE) providing a wide range of essential tools for Python developers, tightly integrated to create a convenient environment for productive Python, web, and data science development.

Step 3: Python library Installation

Python library is a collection of related modules of various libraries required to install as:

- Pillow: Provide facility to deal with Images
- OpenCV: It is helpful to perform image processing
- Numpy: A popular machine learning library that supports large matrices and multi-dimensional data and consists of many mathematical functions.
- Tkinter: This library helps create a GUI through Python.
- matplotlib: This library is responsible for plotting numerical data, that's why it is used in data analysis.
- MySql Connector: Provide facility to connect with SQL database in Python

The screenshot showing the Mysql connector installation in the command prompt is given below.

```

C:\WINDOWS\system32\cmd.exe - pip install mysql-connector-python
Microsoft Windows [Version 10.0.19044.1826]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user>PIP INSTALL MYSQL CONNECTOR
ERROR: unknown command "INSTALL" - maybe you meant "install"



C:\Users\user>pip install mysql-connector-python
Collecting mysql-connector-python
  Downloading mysql_connector_python-8.0.30-cp39-cp39-win_amd64.whl (7.8 MB)
    |██████████████████████████████████████████████████████████████████████████████| 7.8 MB 1.3 MB/s
Collecting protobuf<=3.20.1,>=3.11.0
  Downloading protobuf-3.20.1-cp39-cp39-win_amd64.whl (904 kB)
    |██████████████████████████████████████████████████████████████████████████████| 904 kB 467 kB/s
Installing collected packages: protobuf, mysql-connector-python

```

IV. RESULTS AND ANALYSIS**A. Results**

After the experimental setup, the experiments have been performed as per our proposed model, and obtained experimental results are tabulated in table I.

Table I. Shows the experimental results based on parameters used cover image, number of biometric data, share size

Original (Cover Image1)	One part of the Meaningful Share Information		
	No. of Biometric data Contains (Information)	Dimension (In Pixels)	Size (In bytes)
 Dim:275x354 Size: 160,800 bytes	2	275 X 354	202,692
	3	275 X 354	202,806
	4	275 X 354	202,760
	5	275 X 354	202,805
Original (Cover Image2)  Dim: 275x354 Size: 27,626 bytes	2	275 X 354	196,537
	3	275 X 354	196,531
	4	275 X 354	196,676
	5	275 X 354	196,668

The MSE and PSNR values are calculated according to the number of biometric information contained in the share tabulated in table II.

Table II. Calculated MSE and PSNR values with number of biometric information contained in the share

Number of biometric information	MSE	PSNR (In dB)
2	43.89005307310392	31.70714254861346
3	43.95590138674884	31.700631704763993
4	43.95726416709468	31.70049706099805
5	43.88190035952748	31.707949339026683
Extracted Secret Data	0	Infinite
2	41.76141756548536	31.923051287659664
3	41.85010785824345	31.91383779251186
4	41.9381783941106	31.904707981283543
5	41.8774661872967	31.91099964226083
Extracted Secret Data	0	Infinite

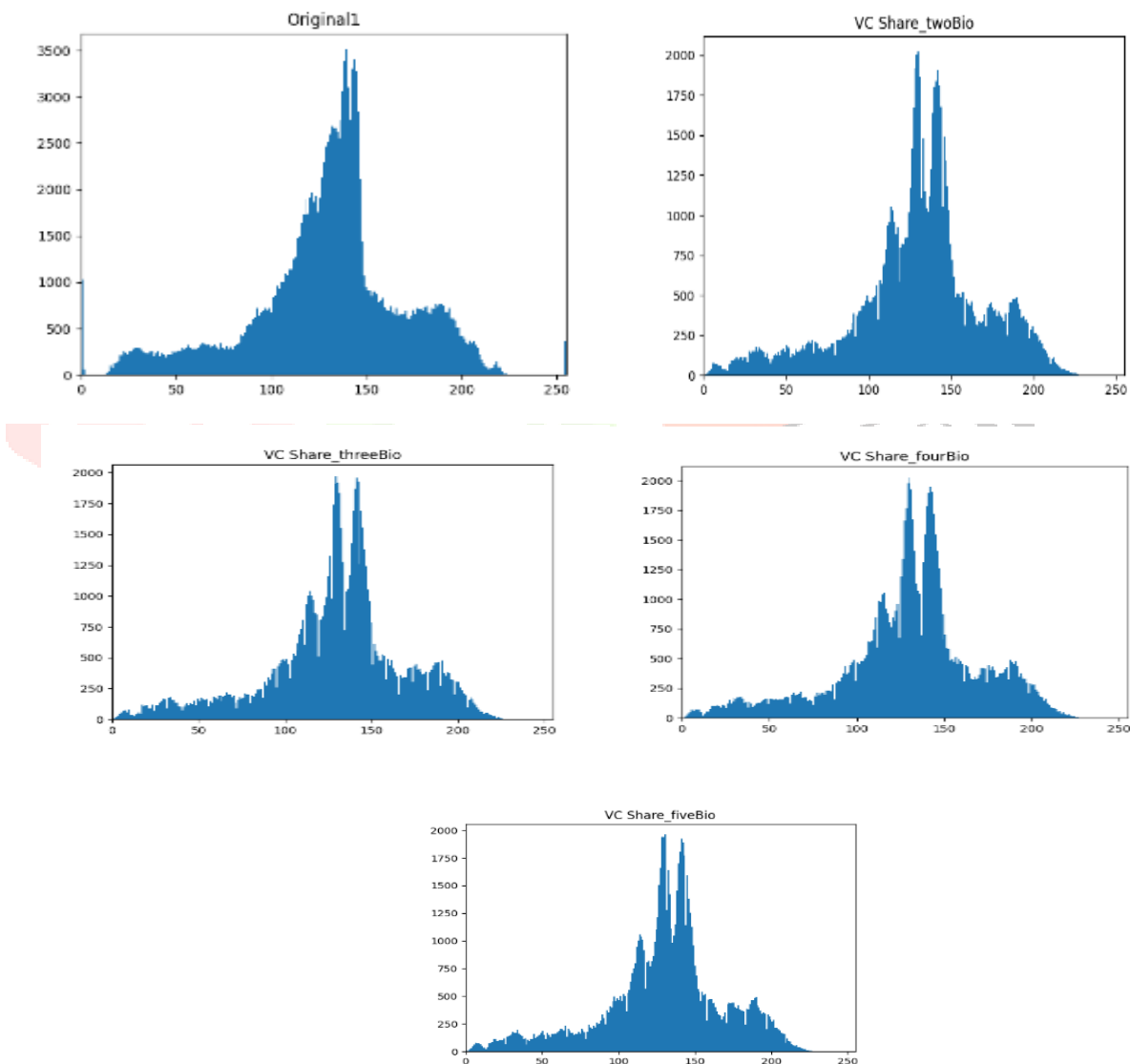


Fig. 4. Histogram of original (cover image1) with the meaningful shares containing a different number of family member's biometric information

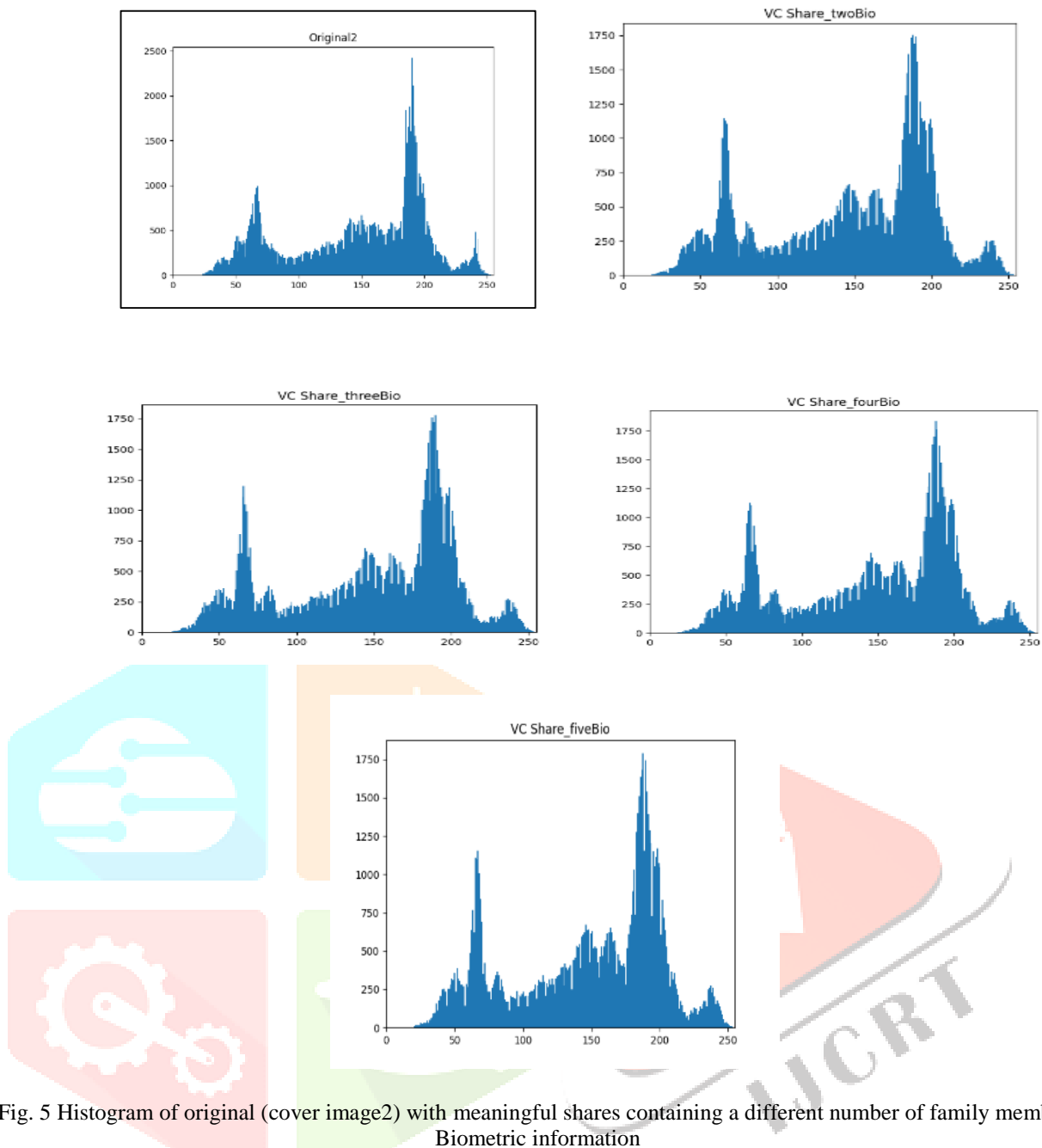


Fig. 5 Histogram of original (cover image2) with meaningful shares containing a different number of family member's Biometric information

While examining the histograms of an original cover image1 and cover image2 concerning their meaningful generated share, slight deviations in the histograms are noticeable. This histogram provides a cumulative value for all three colors channels (red, green, and blue) at each brightness level (0-255).

In the above histograms,

- i. Many differences have been seen between original and VC shares because the original image contains data up to 4 LSB bits in our algorithm and the data loss is too high.
- ii. If we compare two successive share images, then a slight difference is seen in their intensity because one secret image size increases than the original image.
- iii. If we compare the first and last VC shares, then significant deviation has been seen between them.

Therefore, we can conclude that as the number of secret images increases, the intensity value of an original image decreases due to the data embedded in the original image. In the case of vector images, there is less loss of pixel data if the size is large; if you work with PNG or JPEG images, then a few amounts of variation in the size of images that have been seen. With the advent of the shared key concept, the security of the visual cryptography process has been enhanced. The shares are allowed to be dispatched over the same channel or through different channels parameters such as Mean Square Error (MSE) and Peak Signal Noise Ratio (PSNR) are used to judge the optimality of the proposed scheme.

$$PSNR = 10 \log_{10} \frac{(L - 1)^2}{MSE}$$

Where,

Mean Square Error (MSE): The MSE is defined as the difference between the pixel value of the decrypted image and the original image.

$$MSE = \frac{1}{MN} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (O(i,j) - D(i,j))^2$$

As PSNR is the inverse function of MSE, thus the high value of PSNR is preferable because the ratio of signal to noise is high, Where 'signal' is the original image, and the 'noise' is the reconstruction error, a scheme with lower MSE and higher PSNR is ideal.

V. CONCLUSION

We implemented the proposed model using security schemes such as steganography and visual cryptography and found that we can easily control the bogus ration cards and minimize the leakage of food grains through smart ration cards. The main advantage of using this card is that it removes the dependency on another card, such as an Aadhar card. The same mechanism can also be used for implementing any other scheme to provide security for biometric information. The following suggestions for the future:

1. We can also use QR codes and digital chips to access the shares.
2. We can use face recognition algorithms to verify a family member.

REFERENCES

- [1] Ross, A., and Othman, A., "Visual cryptography for biometric privacy," International Journal of IEEE transactions on information forensics and security, Vol. 6(1), pp.70-81, 2010.
- [2] Dickman, Shawn D., "An overview of steganography," Department of Computer Science, James Madison University Infosec Techreport, Vol. 2, pp. 305-315, 2007.
- [3] Bhakta, Anupam, et al., "An Approach of Visual Cryptography Scheme by Cumulative Image Encryption Technique Using Image-key Encryption BitSieved Operation and KN Secret Sharing Scheme," International Journal of Innovative Technology and Exploring Engineering, Vol.3 (1), pp. 20-23, 2013,
- [4] Aarti, Pushpendra K. Rajput, "An EVCS for Color Images with Real Size Image Recovery and Ideal Contrast Using Bit Plane Encoding," International Journal of Computer Network and Information Security, Vol 2, pp.54-60, 2014.
- [5] Kannoja Suresh Prasad, and Jasvant Kumar, "XOR-based unexpanded meaningful visual secret sharing scheme," International Journal of Secure Networks, Vol.14(1), pp. 1-9, 2019.
- [6] Jeyavadhanam, B. Rebecca, and B. Angel Rubavathy, "Visual Cryptography for Biometric Privacy, Authentication and General Access Structure: A Review".
- [7] Sahai, Shubham, and Arvind Kumar Singh, "Visual Cryptography Based Secure Transactions in e-banking "
- [8] Singh Amritpal, and Harpal Singh, " An improved LSB based image steganography technique for RGB images," International conference on electrical computer and communication technologies, 2015.
- [9] Suganya, M., and K. Krishnakumari, "A novel retina-based biometric privacy using visual cryptography," International Journal of Computer Science and Network Security, Vol.16(9), pp. 76, 2016.
- [10] Suganya, M., and S. Suganya, "A Fingerprint Biometric Privacy Using Visual Cryptography," 2017.
- [11] Verma, Jagdeep, and Vineeta Khemchandani, "A visual cryptographic technique to secure image shares," International Journal of Engineering Research and Applications, Vol.2 (1) pp.1121-1125, 2012.
- [12] Kuri, Ms. Moushmee, and Dr. Tanuja Sarode, "RKO Technique for Color Visual Cryptography," IOSR Journal of Computer Engineering, e-ISSN: 2278-0661.
- [13] Revenkar, Pravin S., Anisa Anjum, and W. Z. Gandhare, "Survey of visual cryptography schemes," International Journal of Security and Its Applications, Vol. 4(2), pp. 49-56, 2010.
- [14] Sharma, A. and D. K. Srivastava", A comprehensive view on encryption techniques of visual cryptography," International Journal of Recent Research and Review, Vol.7(2), 2014.
- [15] Ibraheem, Noor A., et al., "Understanding color models: A review," ARPN Journal of Science and Technology, Vol 2(3), pp. 265-275, 2012.
- [16] Jyoti Tripathi, Anu Saini, Kishan, Nikhil, Shazad, "Enhanced Visual Cryptography: An Augmented Model for Image Security," Procedia Computer Science, Vol.167, pp.323-333, ISSN 1877-0509, 2020.

Mr. Manish Prajapati pursued a Bachelor of Science from the University of Lucknow, Lucknow, in 2020. Now pursuing a Master of Science in Computer Science at the University of Lucknow, Lucknow. Manish's area of research interest is to work on real-time projects, such as computer vision, cryptography algorithms, network security, and cloud security.

Suresh Prasad Kannoja has been working as an assistant professor in the Department of Computer Science, University of Lucknow, Lucknow, since 2005. He completed his Ph.D. in 2013 from the University of Lucknow, Lucknow. His current area of research interest includes image classification, software quality, system security, soft computing, visual cryptography, and network security. He has also organized three national conferences and one national research scholars meet. He has published 22 research papers in national and international journals/conferences.

