ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

Data Security and Payment System using Mod-4 LSB and Visual Cryptography

Suman. V. Nandyal, Binu Singh

M. Tech, Dept. of ECE, NMIT, Bengaluru, India

Assistant Professor, Dept. of ECE, NMIT, Bengaluru, India

ABSTRACT: Data safety has become a major problem in data communication especially in the field of computer network. AES algorithm has been adapted to increase the security for the data. Mod-4 LSB algorithm is used for the embedding. The data can have many forms such as text, image and audio etc. There are a lot of cryptosystems exists to preserve data; out of those Half Tone Visual Cryptography (VC) is one of the popular approaches to preserve image based information. It splits the key image into shares in encryption procedure and the long-established image can also be retrieved by using stacking the specified number of shares at the time of decryption. Steganography is an additional approach of cryptosystem used to protect information. It hides the secret in another data. This paper presents a brand new strategy for delivering restrained information only that is vital for fund transfer during online browsing thereby safeguarding customer data and increasing confidence.

KEYWORDS: AES, Half Tone Visual Cryptography, Integer Wavelet Transform, Mod-4 LSB.

I. INTRODUCTION

With the development of e-commerce, payment systems and protocols have been developed. The current payment system consists of merchants, consumers and transaction portals such that a merchant receives a consumer’s payment information and forwards it to a payment portal to process the payment. This, however, exposes a consumer’s payment information to risks, because a merchant can save the consumer’s payment information in either plain or encrypted form and may misuse it later. It is also possible that a merchant’s server, through which a consumer’s payment information is forwarded to a payment portal, is compromised and the merchant is unaware of it.

With the explosive development of internet in recent years the security and the confidentiality of the sensitive information has become of prime and utmost significance and concern. To protect this information from unauthorized access and tampering various methods for information hiding like, hashing, cryptography and authentication have been established. In this paper we will discuss one such information hiding technique called Steganography [10]. Steganography is the process of masking sensitive information in any media to transfer it securely over the underlying unreliable and insecure communication network.

Visual cryptography (VC) is a method of encrypting a secret image into shares such that stacking a sufficient number of shares reveals the secret image. Visual cryptography (VC), proposed by Naor and Shamir, is a method for protecting image-based secrets that has a computation-free decryption process. In the (2, 2) VC scheme each secret image is divided into two shares such that no information can be reconstructed from any single share. Each share is printed in transparencies. The decryption is achieved by stacking the two shares and the secret image can be visualized by naked eye without any complex cryptographic computations.

The selling and buying of goods and facilities over the Internet is known as electronic commerce (e-commerce). The concept of e-commerce is, however, not just limited to buying and selling of goods. It also includes the entire purchase process of developing, marketing, vending, supplying, servicing and paying for products and services.

In that case, if a merchant’s server or system is not secure enough to prevent intrusion of data stealers, spammers, spyware, malware and hackers, consumer data may be stolen and misused. Hence, to avoid the issue of data mishandling or unsecured data on the merchant side, we propose a payment method that does not send consumer payment information to merchants and allows only payment portal to deal with it. Payment portal are secure and reliable, because they comply with the standard data security rules and communicate with banks and credit card companies using the most secure methods and technologies. To strengthen data security, the implemention of a new payment portal scheme is introduced along with visual cryptography & steganography in our proposed online payment system.

II. Related Work

We have studied many previous works done in this field by different researchers. There are many approaches that were followed by different researchers. S. R. Navale et al [1] proposed a new approach for online transaction in which a consumer's payment information is minimized to that is only needed for transfer of funds. They used the text steganography and visual cryptography to securely transfer funds to a merchant and protect a consumer's payment data from any Internet susceptibilities.

Pratiksha P.Patil and Y.M. Patil [2] proposed an extended visual cryptography to construct meaningful binary images as shares, but the visual quality is poor. So, a technique named halftone visual cryptography is implemented to achieve visual cryptography via half toning. This method utilizes the void and cluster algorithm to encode a secret binary image into halftone shares (images) carrying significant visual information. M.Vijay and V. VigneshKumar [3] proposed a system, where Integer Wavelet Transform is performed on a gray level cover image and in turn embeds the message bitstream into the LSB's of the integer wavelet coefficients of a the image . The main purpose of the proposed work is to focus on improving embedding capacity and bring down the distortion occurring to the stego image. Chandra Prakash Shukla et al [4] proposed a methodology which combines steganography and cryptography to enhance the security of message. Do Van Tuan [5] presented a new scheme for embedding secret data into a binary image. For each block of m × n pixels, the new scheme can hide $\lfloor log_2(m \times n + 1) \rfloor$ bits of data by changing one bit at most in block.

Komal Patel, Sumit Utareja and Hitesh Gupta [6] presented a survey on various information hiding techniques in steganography and evolution of different existing image steganography techniques of information hiding and concluded that researches and gave some advantages and disadvantages. N.Santoshi, B.Lokeswara Rao and B.Lokeswara Rao [7] proposed an adaptive steganography scheme. The adaptive quantization embedded is introduced and employed by block-wised fashion. They also constructed contrast-correlation distortion metric to optimally choose quantization steps for image blocks to guarantee more data being embedded in busy areas.

III. Proposed System

The Block diagram of proposed work is shown in the figure 1 and figure 2. The detailed explanation of the proposed work is given below.

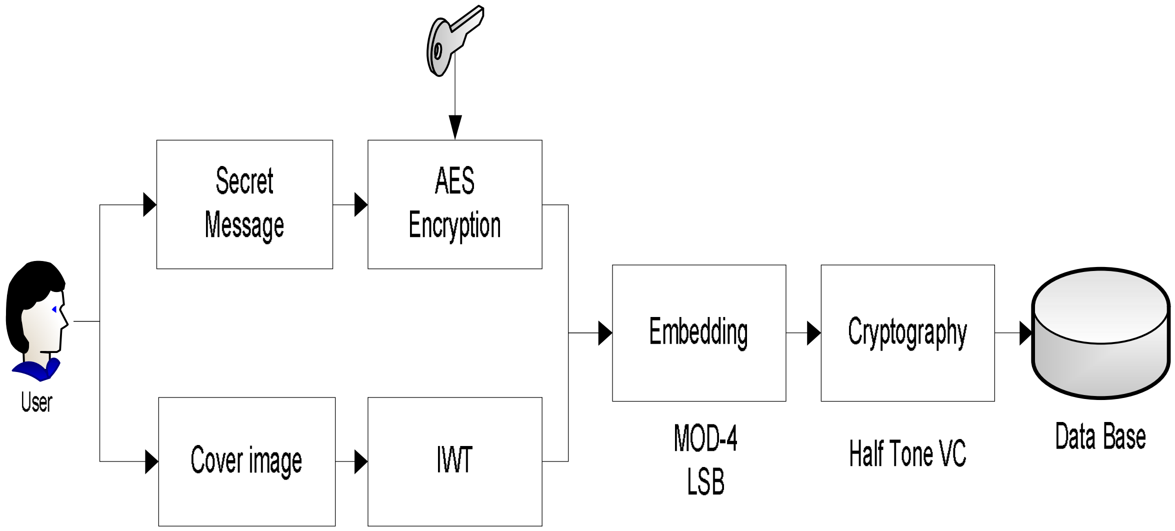


Figure 1: Block Diagram of Embedded Process

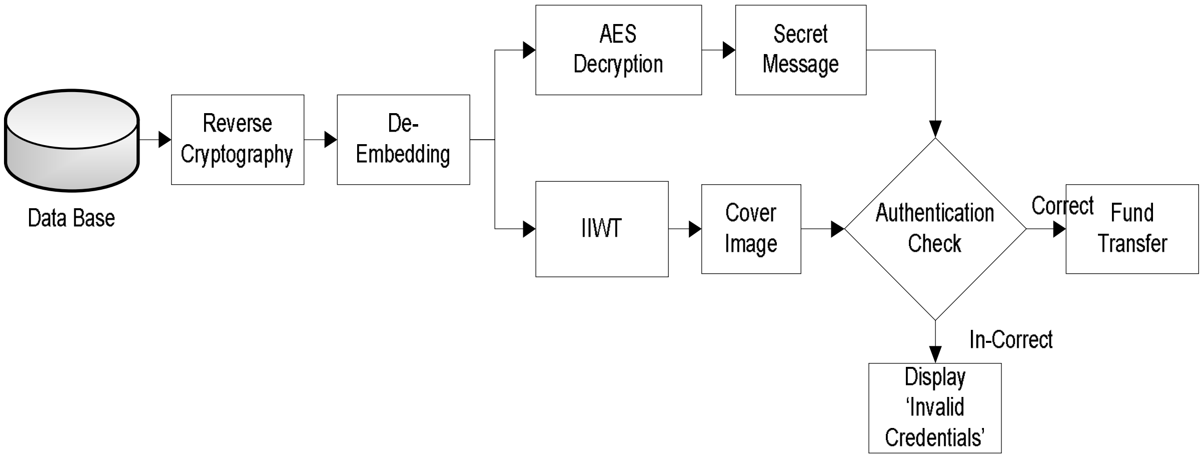


Figure 2: Block Diagram of De-embedded and Authentication Process

A. AES Approach:

Encryption is an approach of obscuring information to make it unreadable without desirable knowledge. Encryption has been used to protect communications for centuries, but only organizations and individuals with an extraordinary need for secrecy had made use of it. In the mid-1970s, strong encryption approach emerged from the sole preserve of secretive govt corporations into the general public domain, and is now used in protecting widely-used systems, such as internet e-commerce, mobile telephone networks and bank automated teller machines. Encryption can be used to ensure secrecy.

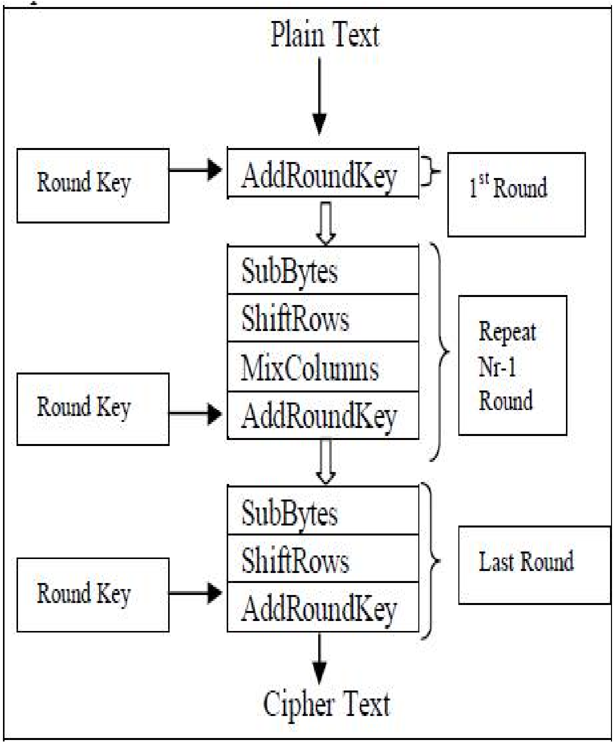


Figure 2 AES Encryption Process

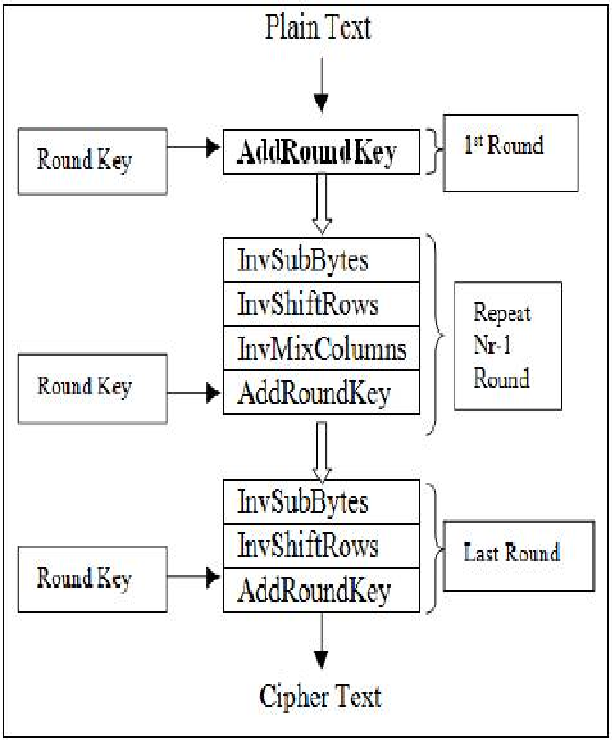


Figure 3 AES Decryption Process

The input (block size N_b, also known as plaintext) of the AES algorithm is converted into a 4 x 4 array, called a state. Four transformations, AddRoundKey, SubBytes, ShiftRows and MixColumns, perform various operations on the state to calculate the output state (the final cipher text). Except for AddRoundKey each of these operations are invertible. To perform all these transformations above, some mathematical operations are needed to understand. Figure 2 and 3 show the encryption and decryption process.

B. Integer Wavelet Transform (IWT)

The proposed algorithm employs the wavelet transform coefficients to embed messages into four sub bands of two dimensional wavelet transform. To avoid issues with floating point precision of the wavelet filters, we used Integer Wavelet transform. The LL sub band in the case of IWT appears to be a close copy with of the normal image at the same time in the case of DWT the resulting LL sub band.

Lifting Scheme is one of the techniques on integer wavelet transform. The decomposing filter in integer wavelet transform can be calculated using eq. (1)

$$S_{1,k} = \lfloor (S_{0,2k} + S_{0,2k+1})/2 \rfloor \qquad (1)$$

$$d_{1,k} = S_{0,2k+1} - S_{0,2k} \qquad (2)$$

The inverse transform can be calculated using eq. (3) and (4)

$$S_{0,21} = S_{1,1} \lfloor d_{1,1}/2 \rfloor \qquad (3)$$

$$S_{0,21+1} = A_{1,1} + \lfloor (d_{1,1} + 1)/2 \rfloor \qquad (4)$$

C. Embedding: Mod-4 LSB Embedding

Several versions of LSB insertion exist. It is possible to use a random number generator initialized with a Stego-key and its output is combined with the input information, and this is embedded to a cover image. For example in the presence of active warden it's not ample to embed a message in a recognized location (or in a known sequence of bits) when you consider that the warden is equipped to change these bits, despite the fact that he can't make a decision whether there is a secret message or not, o r he can't read it when you consider that it is encrypted. The usage of a stego-key is important, considering the fact that the security of a protection approach must not be based on the secrecy of the

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

algorithm itself, instead of the option of a secret key. Here two bits of secret message are embedded in to the cover image at a time, so it takes four iterations to embed the first 8 bit of message. Hence the name Mod-4 LSB approaches.

D. *Half-Tone Visual Cryptography:*

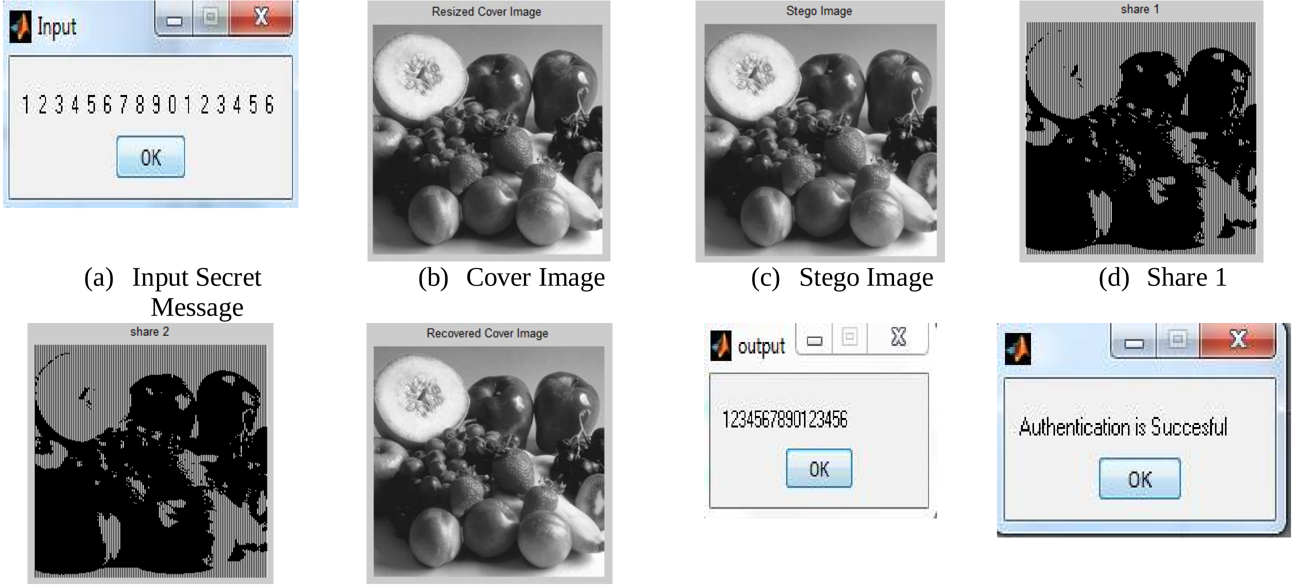
In a 2-out-of-2 halftone [10] visual threshold scheme, a halftone image I, obtained by any halftoning method on a grey level image GI, is assigned to participant 1. Its complementary image $\check{I}$, obtained by reversing all black/white pixels of I to white/black pixels, is assigned to participant 2. To encode a secret pixel p into a $Q_1 \times Q_2$ halftone cell in each of the two shares, only 2 pixels, referred to as the secret information pixels, in each halftone cell need to be modified. The two secret information pixels should be at the same positions in the two shares. If p is white, a matrix M is randomly selected from the collection of matrices C_0. If p is white, M is randomly selected from the collection of matrices C_1. The secret information pixels in the ith $(i = 1, 2)$ share are replaced with the two sub-pixels in the ith row of M. These modified pixels carry the secret information of the encoded image. The other pixels in the halftone cells that are not modified are called ordinary pixels [9].

IV. Extraction and Authentication

Extraction includes AES decryption where the cipher text will be decrypted from de-embedded image. Inverse integer wavelet transform is applied to Stego image to get the original image. Once we obtain the plain text after decryption, original message has to be compared with extracted message.

V. Results and Discussion

Figure 2 shows the results of our proposed work; here we set standard PIN 1234567890123456 which acts as secret message. In the simulation work we used manual pin num which is compared with the extracted message and authenticates. Initially secret message (input) is embedded in cover image shown in figure (b) using Mod-4 LSB algorithm, resultant embedded image is shown in the figure (c), then shares are generated figure (d) and (e) using half tone cryptography approach. After de-embedding we recover both secret message and cover image as shown in the figure (f) and (g) and compare the extracted message with the set pin in the database. if both input image extracted message match with pin then it displays 'Authentication Successful', else 'Invalid Credentials!, Pls Try Again Later'.



1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6

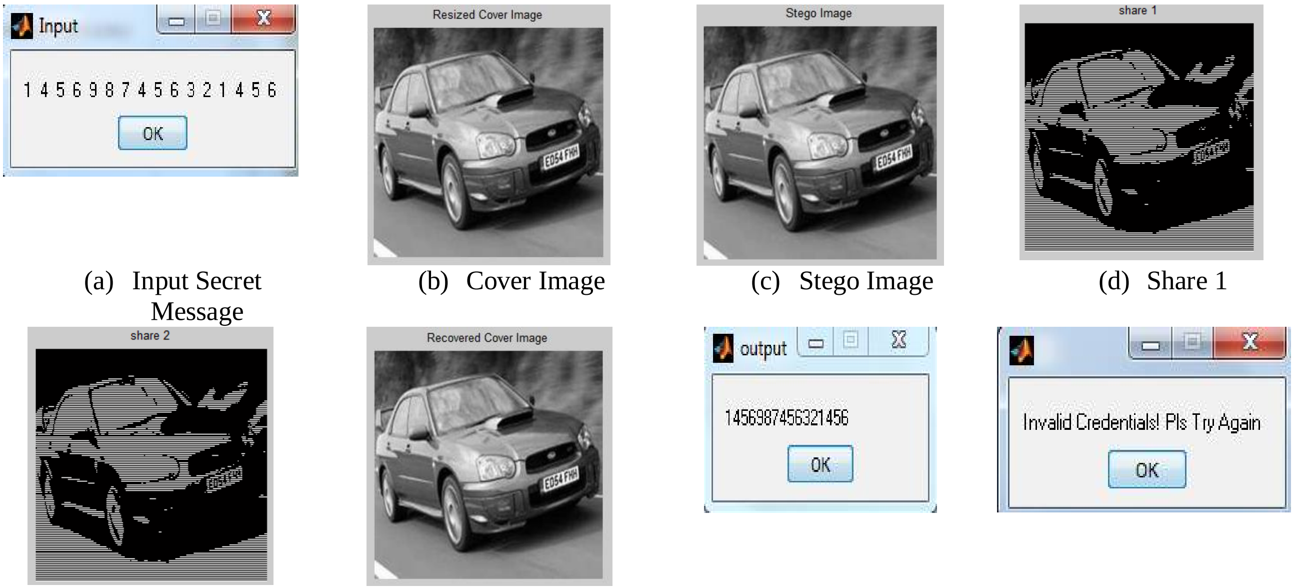
1234567890123456

Authentication is Succesful

(a) Input Secret Message (b) Cover Image (c) Stego Image (d) Share 1

(e) Share 2 (f) Recovered Image (g) Extracted Secret Message (h) Authentication Result

Figure 2: Experimental Result of Proposed Work



1 4 5 6 9 8 7 4 5 6 3 2 1 4 5 6

1456987456321456

Invalid Credentials! Pls Try Again

(a) Input Secret Message

(b) Cover Image

(c) Stego Image

(d) Share 1

(e) Share 2

(f) Recovered Image

(g) Extracted Secret Message

(h) Authentication Result

Figure 3: Result2 of our Proposed Work

VI. Conclusion

In this paper we presented an approach which uses combined steganography and cryptography to increase the security of data. Mod-4 LSB technique has been used which efficient and less time consuming. Half tone visual cryptography is used as a cryptographic method. Based on the results obtained after inverse process, authentication has been done.

References

[1] S. R. Navale, S. S. Khandagale, R. A. Malpekar and N. K. Chouhan, “Approach for Secure Onlinetransaction using Visual Cryptography & Text Steganography”, International Journal of Engineering Research & Technology (IJERT), Volume 4 Issue 03, 2015.

[2] Pratiksha P.Patil and Y.M. Patil, “Visual Cryptography Based on Halftoning”, Journal of Electronics and Communication Engineering, pp 65-69.

[3] M.Vijay, V. VigneshKumar, “Image Steganography Method Using Integer Wavelet Transform”, International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Issue 3, 2014.

[4] Chandra Prakash Shukla, Ramneet S Chadha and Abhishek Kumar, “Enhance Security in Steganography with cryptography”, International Journal of Advanced Research in Computer and Communication Engineering Volume 3, Issue 3, 2014.

[5] Do Van Tuan, Tran Dang Hien and Pham Van At, “A Novel Data Hiding Scheme for Binary Images”, International Journal of Computer Science and Information Security, Volume 10, Issue 8, 2012.

[6] Komal Patel, Sumit Utareja and Hitesh Gupta, “A Survey of Information Hiding Techniques”, International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 1, January 2013.

[7] N.Santoshi, B.Lokeswara Rao and B.Lokeswara Rao, “A Secure and Lossless Adaptive Image Steganography with Mod-4 LSB Replacement Methods Using Image Contrast”, International Journal of Scientific & Engineering Research, Volume 3, Issue 8, 2012.

[8] Zhongmin Wang, Gonzalo R. Arce and Giovanni Di Crescenzo, “Halftone Visual Cryptography via Direct Binary Search”, 14th European Signal Processing Conference (EUSIPCO 2006), 2006.

[9] Zhi Zhou, Gonzalo R and and Giovanni Di Crescenzo, “Halftone Visual Cryptography”, IEEE Transactions on Image Processing, Volume 15, Issue 8, 2006.

[10] Prateek Kumar, Suneeta Agarwal and Shivendra Shivani, “Halftone Visual Cryptography with Pixel Expansion through Error Diffusion”, International Journal of Information & Computation Technology, Volume 4, Issue 14 (2014).