UNIVERSITÀ DEGLI STUDI DI BRESCIA

DII, COMMUNICATION TECHNOLOGY & MULTIMEDIA

DIGITAL IMAGE PROCESSING

A NEW ROBUST WATERMARKING SCHEME FOR COLOUR IMAGE IN SPATIAL DOMAIN

BY:

1. ALEMU SISAY NIGRU
2. GIRMA TARIKU WOLDESEMAYAT
3. KASSAHUN MAMUYE TESFAYE

OUTLINE

- INTRODUCTION
- PROBLEM STATEMENT
- A HIGH-LEVEL DESCRIPTION OF THE METHOD
- PROVIDED RESULTS AND DISCUSSION
- CONCLUSION

INTRODUCTION

- **Digital watermarking** is a technique to hide the copyright information into the digital data through certain algorithm.
- The watermark:
  1. is embedded into the host media to be protected, such as an image, audio or video.
  2. can be **detected** or **extracted** later to make an assertion about the host media.
  3. should not alter the quality and visually of the host image and it should be **perceptually invisible**.
  4. **robust** with respect to image distortions, i.e.
     - difficult for an attacker to remove
     - robust to common image processing and geometric operations, such as filtering, resizing, cropping and image compression.

WATERMARKING TECHNIQUES

SPATIAL DOMAIN

- The watermark embedding is achieved by directly modifying the pixel values of the host image.
- The least significant bit of each pixel in the host image is modified to embed the secret message.
- The watermark is embedded in saturation on the HIS(hue, saturation, intensity) colour space.
- The watermark is embedded into dc components of colour image directly.
- Embedding the watermark into the original image by dividing the original image into different block size and adjusting brightness of a block according to the watermark.

TRANSFORM DOMAIN

- The host image is first converted into frequency domain then, transform domain coefficients are modified by the watermark.
- the watermark is embedded into the DCT coefficients of sub images, which are obtained by subsampling the original image.
- An algorithm based on embedding the watermark image three times in different frequency bands that are low, medium and high;
- Two complementary watermarks can also embedded into the host image in order to make it difficult for attackers to destroy both of them.

….CONT'D

NON BLIND

- Requires original image and secret key for watermark detection

BLIND

- Requires only the secret keys for extraction.

SEMI-BLIND

- Requires secret key and watermark bit sequence for extraction.

PROBLEM STATEMENT

- Most related methods are quite robust against some common image processing operations, such as median filter, scaling and rotation; however, they are **less robust to cropping attack** because the watermark bits are embedded into the whole image hence some data would be lost in cropping.
- The embedding process of the related method is done by using convolutional code. But the problem is that it needs a **constant high amount of decoding operations,** even if few or no errors occurred.

WATERMARK EMBEDDING

Embedding Process

H = original image of size 512x512
W = watermark image of size 32x32
K = pseudo random sequence of 32x32

Step 1: Permutation of the watermark image

i. **W'** = **W**$\oplus$ **K** – Xoring

ii. Apply Grade code to **W'** to find the permuted watermark **W''**

Step 2 : Extract the **B** component and divide into non overlapping blocks of size 8*x*8

Step 3 : Determine embedding positions using the private key

WATERMARK EMBEDDING

Step 4: The encoded watermark W'' is embedded in the blue component B. For each encoded watermark bit, a block of 8*8 is modified as follows:

```
IF W''=1;
For all the pixels of the 8*8 blocks
    {I'=I+ λ}
IF W''=0;
For all the pixels of the 8*8 blocks
    {I'=I- λ}
```

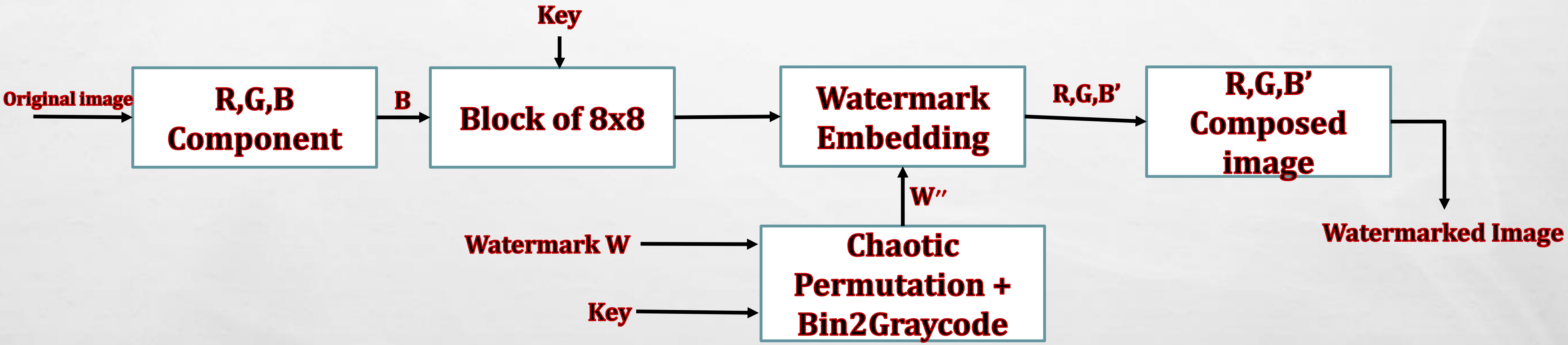
Where I' : modified pixel intensity value

I : original pixel intensity value

λ : constant.

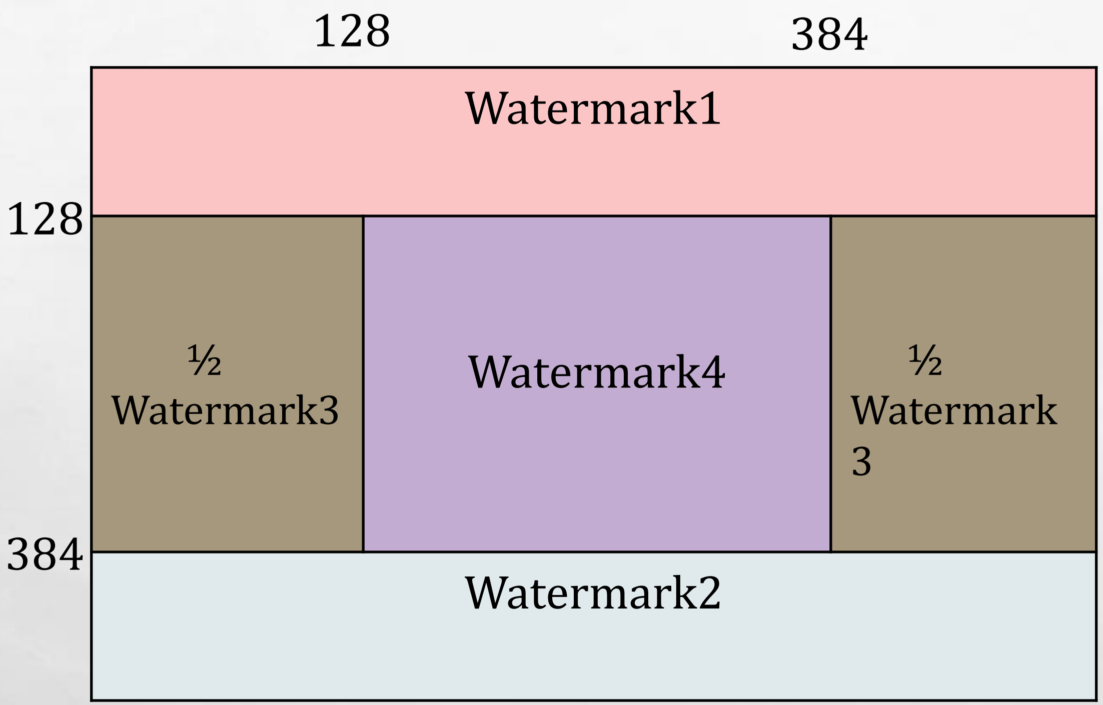
Step 5: The modified block of pixels is then positioned in its original location of the host image image and then step 3 and 4 is repeated until all encoded watermark bits W'' are embedded.

A HIGH-LEVEL DESCRIPTION OF THE METHOD



….. CONT'D

The proposed watermarks embedded positions



128

384

Watermark1

128

½ Watermark3

Watermark4

½ Watermark 3

384

Watermark2

WATERMARK EXTRACTION

Extraction Process

Step 1: Non blind approach. The extraction is based on the probability of detecting bit '**1**' or '**0**' as a result of pixel wise comparison of I and I'

P1=P1+1/64 IF I' > I

P0=P0+1/64 IF I' ≤ I

Step 2: Based on the probability (P1, P0), the extracted watermark bits **W''** can be computed as:

W'' = 1 IF P1 ≥ P0

W'' = 0 IF P1< P0

Step 3: The extracted watermark bits for the four watermarks are decoded using Gray code and then, the decoded bits are XOR with random bits. We obtain images **W'1**, **W'2**, **W'3**, **W'4**.

….CONT'D

Step 4: Compute the normalized cross correlation between **W** and **W'1**, **W'2**, **W'3**, **W'4** to make a binary decision on whether a given watermark exists or not. We choose 0.5 as the threshold for the watermark decision.

$$\boldsymbol{NCC} = \frac{\sum_i \sum_j \boldsymbol{W_{ij} W_{ij}}'}{\sum_i \sum_j (\boldsymbol{Wij})^2}$$

Peak signal to noise ratio can be calculated as:

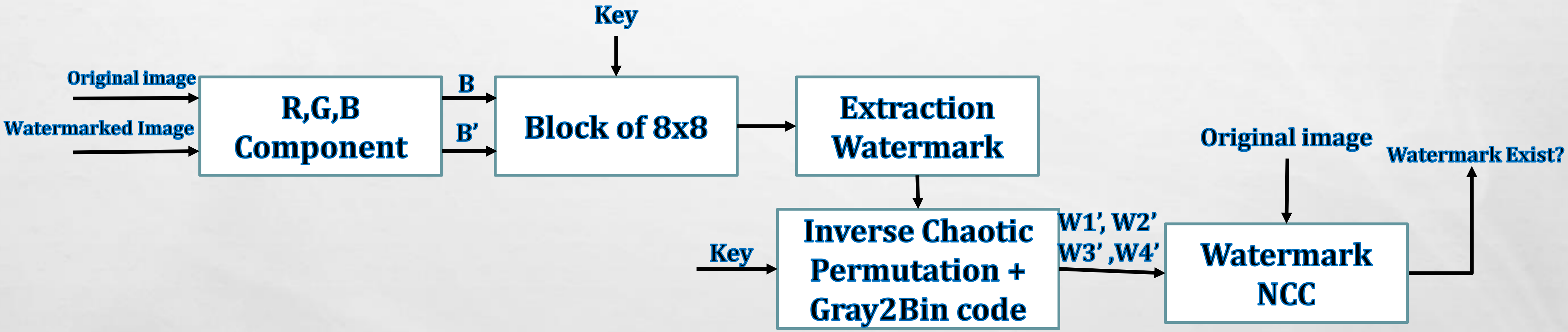
$$\boldsymbol{PSNR = 10 * \log_{10} \frac{255}{MSE}}$$

Where:

$$\boldsymbol{MSE} = \frac{1}{3mn} \sum_{i=0}^{m} \sum_{j=0}^{n} (\boldsymbol{r}[\boldsymbol{i},\boldsymbol{j}] - \boldsymbol{r}'[\boldsymbol{i},\boldsymbol{j}])^2 + (\boldsymbol{b}[\boldsymbol{i},\boldsymbol{j}] - \boldsymbol{b}'[\boldsymbol{i},\boldsymbol{j}])^2 + (\boldsymbol{g}[\boldsymbol{i},\boldsymbol{j}] - \boldsymbol{g}'[\boldsymbol{i},\boldsymbol{j}])^2$$

....CONT'D

- WATERMARK EXTRACTION



RESULTS AND DISCUSSION

1. Watermark Extraction

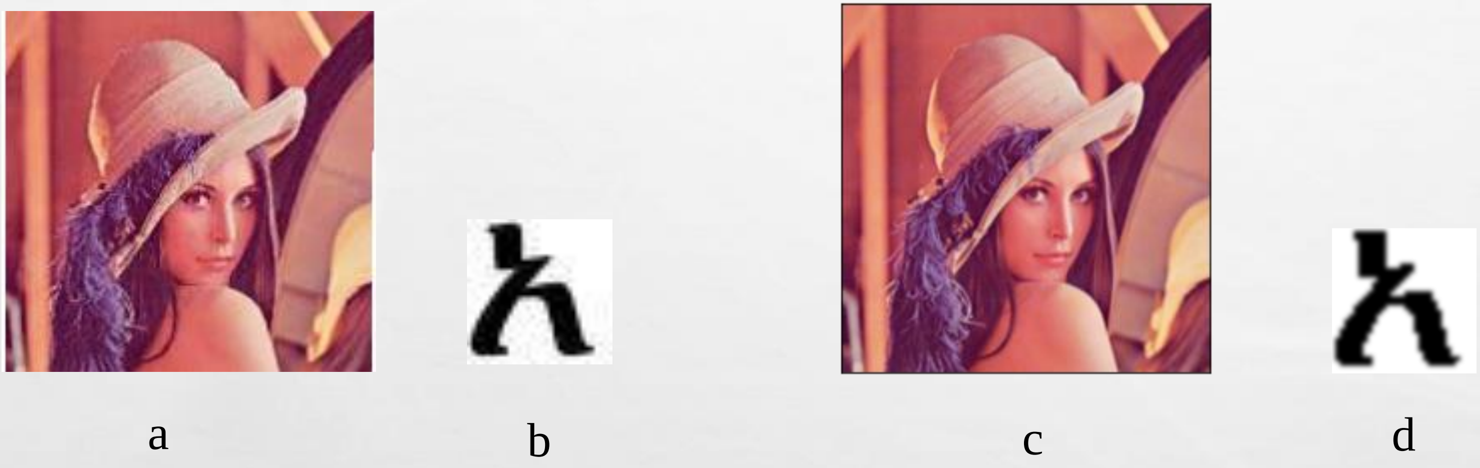


Fig.1. (a) Original image
(b) Original watermark
(c) Watermarked image
(d) Extracted watermark (NCC = 1.0)

….. CONT'D

2. Attack - Compression

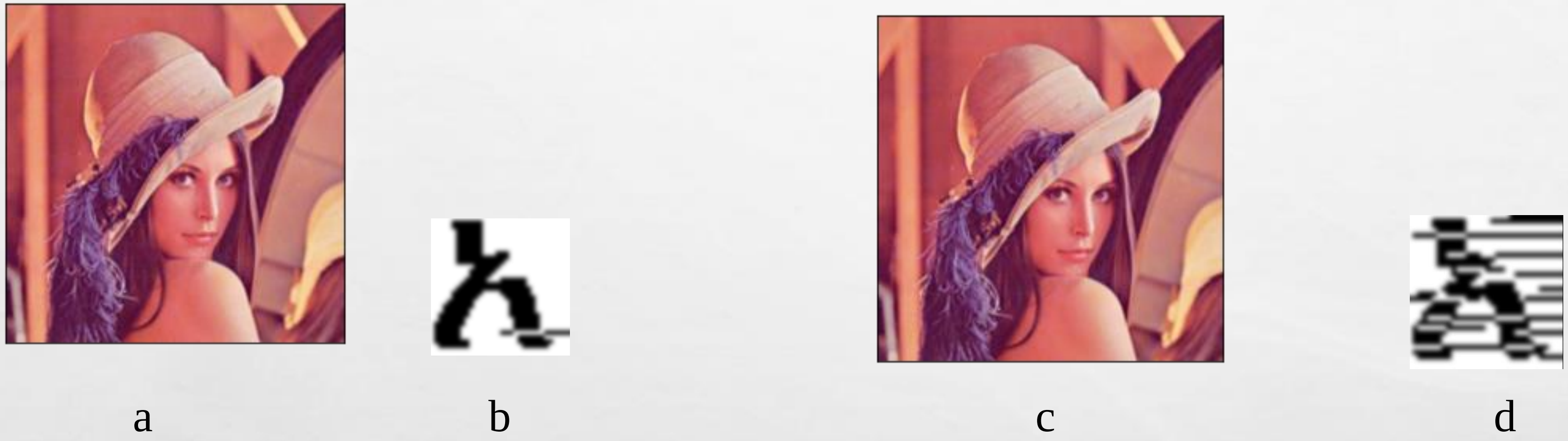


Fig.2. (a) JPEG compressed watermarked Q=75
(b) Extracted watermark NCC=0.9874

(c) JPEG compressed watermarked Q=50
(d) Extracted watermark (NCC = 0.77468)

….. CONT’D

3. Attack - Rotation

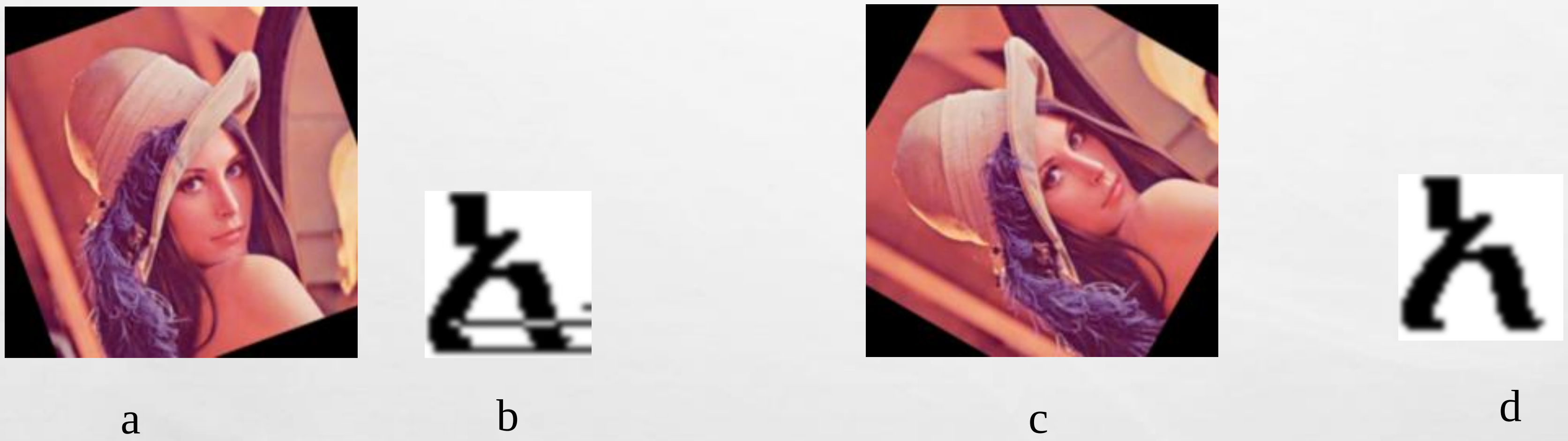


Fig.3. (a) Watermarked image after rotation by 20^0 (c) Watermarked image after rotation by 60^0
(b) Extracted watermark NCC=0.9290 (d) Extracted watermark (NCC = 1.0)

….. CONT’D

4. Attack - Cropping

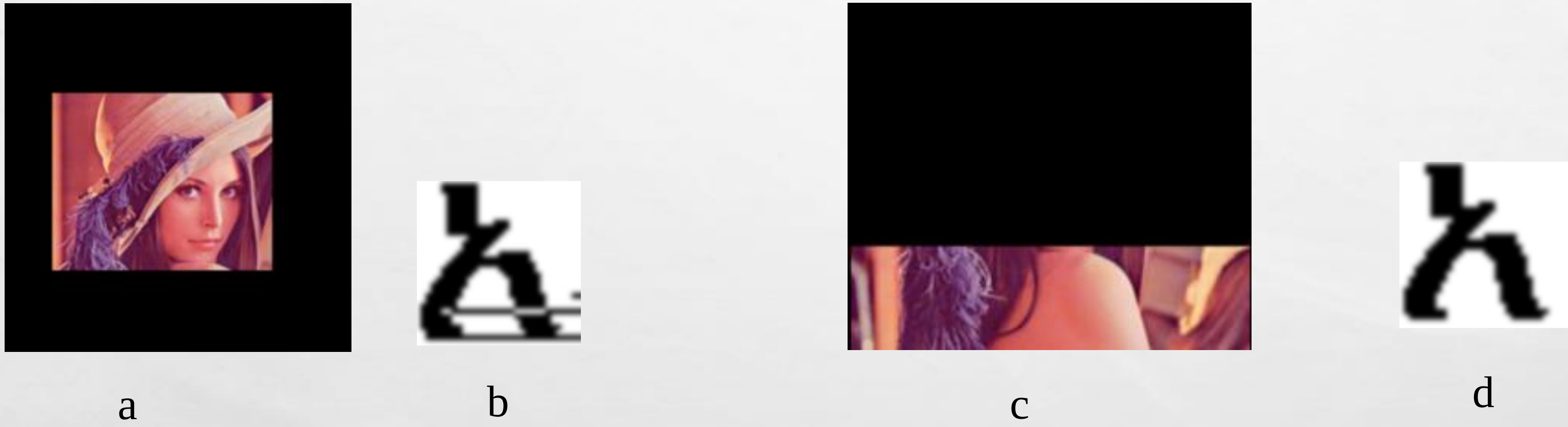


Fig.4. (a) Cropped watermarked by 60%
(b) Extracted watermark NCC=0.9290

(c) Cropped watermarked by 75%
(d) Extracted watermark (NCC = 1.0)

….. CONT'D

5. Attack – Salt and pepper noise

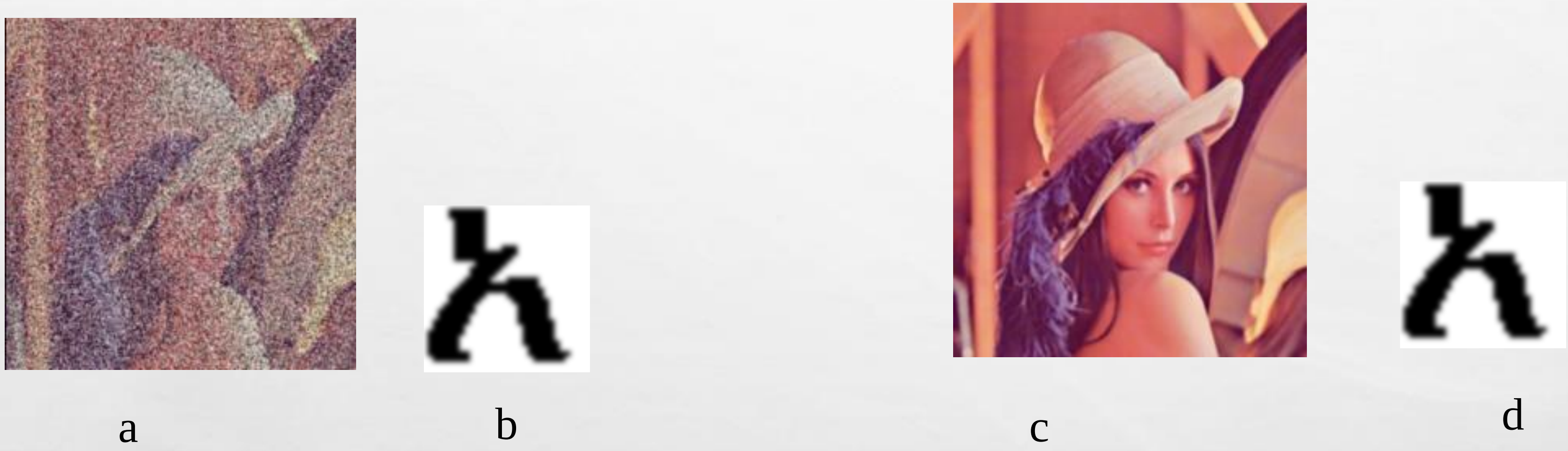


Fig.5. (a) Watermarked image under salt and pepper noise attack (**SNR**=0.4) (c) Watermarked image after filtering
(b) Extracted watermark (NCC = 1.0) (d) Extracted watermark (NCC = 1.0)

CONCLUSION

- The algorithm developed is robust against various types of image processing attacks such as, filtering, cropping, scaling, compression, rotation and salt and paper noise.
- The watermark signature is recovered with higher values of correlation when the watermarked image is attacked.
- It is also secure scheme, only the one with the correct key can extract the watermark.

ANY QUESTION?

THANK YOU!
GRAZIE!
እናመሰግናለን!