Hybrid Method of Edge Detection for Data Hiding Technique of Digital Mammograms

[1]Samya Muhuri, [2]Monalisa Bhattacharjee

M.Tech. Student
Computer Science and Engineering Department,
RCC Institute of Information Technology, Kolkata, India

Abstract - **In the Medical Oncology domain, we were brought to make periodic mammography images to monitor breast tumor patients. This paper proposes a role-based access control framework comprising two main components – a content-based steganographic module and a reversible watermarking module, to protect mammograms in the medical database. The input is a mammogram image and patient's information. Within this framework, the content-based steganographic module is to hide patients' textual information into mammograms without changing the important details of the pictorial contents and to verify the authenticity and integrity of the mammograms. The reversible watermarking module, capable of masking the contents of mammograms, is for preventing unauthorized users from viewing the contents of the mammograms. Identifying only the breast area will be done before the embedding process. To detect breast boundary a novel hybrid algorithm for edge detection has been proposed in this paper. There are large numbers of edge detection operators available, each designed to be sensitive to certain types of edges. Here we present the hybrid of Fuzzy and Canny edge detection technique. The above mentioned processes are tested on different mammographic images randomly retrieved from popular search engine and work has been implemented by MATLAB R2009b package.**

Index Terms— **Steganography, Watermarking, Edge Detection, Canny & Fuzzy Edge Detector.**

I. INTRODUCTION

Breast cancer has been one of the major causes of death among women since the last decades. This disease became a most common cancer among women. If the cancer can be detected early, the options of treatment and the chances of total recovery will increase. Digital mammography screening is performed to detect early stages of breast cancers among women. The screening process produces large amount of digital data of which privacy and security need to be ensured. A picture archiving and communication system (PACS) integrates imaging modalities and acts as the interface between hospitals and departmental information systems in order to manage the storage and distribution of images to radiologists, physicians, specialists, clinics, and imaging centers. This paper proposes a role-based access control framework comprising two main components – a content-based steganographic module and a reversible watermarking module, to protect mammograms on PACSs. Within this framework, the content-based steganographic module is to hide patients' textual information into mammograms without changing the important details of the pictorial contents and to verify the authenticity and integrity of the mammograms. The reversible watermarking module, capable of masking the contents of mammograms, is for preventing unauthorized users from viewing the contents of the mammograms. The scheme is compatible with mammogram transmission and storage on PACSs. In this paper, we present a new approach for watermarking of digital mammographic images. Hence, by identifying best location on the mammogram to embed the patient's information without affecting the quality of the image will be studied. To identify best location (breast boundary) for hiding information, we would use hybrid edge detection technique. Here, Image Watermarking using least significant bit technique has been used for embedding the message into the mammogram images.

Since there are many advantages of medical images are discovered and it is frequently used in the medical domain, most hospitals are facing with issues to manage large amount of data storage such as administrative document, patient's information and medical images. Therefore, it is important to handle those data accurately to avoid problem of lost, tampering and mishandling record at the hospital. We need to ensure the medical information remained unchanged throughout the protection and authentication process in order to avoid any chances of mistakes made in the diagnosis and prognosis process. Digital watermarking is one of the proposed solutions for copyright protection of multimedia data.

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. Watermarking is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to contain a relation to the carrier signal. Watermarking techniques are divided in two categories. Spatial Domain Watermarking, where the least significant bits is replaced with watermark, and Frequency domain watermarking, where the image is first transformed to frequency domain and then the low frequency components are modified to contain the watermark. The best known Watermarking method that works in the Spatial Domain is the Least Significant Bit (LSB) [9]. This method has several implementation versions that improve the algorithm in certain aspects. In this paper we use LSB watermarking technique for hide the mammogram information.

II. Basic Model of Watermarking

Basic model of watermarking [8] with four stages as shown in figure 1.

- Generation
- Embedding
- Distribution and attacks
- Detection and Recovery.

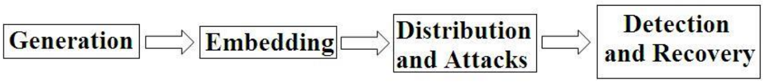


Fig.1. Block Diagram of Watermarking Technique

In Generation stage watermark is created and its contents should be unique and complex such that it is difficult to extract or damaged from possible attacks. In Embedding stage watermark is embedded in cover media. Embedding is directly related to extraction algorithm. The Distribution process can be seen as transmission of signal through watermark channel. Possible attacks in broadcast channel may be intentional or accidental. Detection process allows owner to be identified and provides information to the intended recipients.

Least Significant Bit (LSB) Watermarking Technique

In this paper we present LSB watermarking technique and it was known as image downgrading. An example of the less predictable or less perceptible is Least Significant Bit insertion. This section explains how this works for an 8 bit gray scale image and the possible effects of altering such an image. The principle of embedding is fairly simple and effective. If we use a gray scale bitmap image, which is 8- bit, we would need to read in the file and then add data to the least significant bits of each pixel, in every 8-bit pixel. In a grayscale image each pixel is represented by 1 byte consist of 8 bits. It can represent 256 gray colors between the black which is 0 to the white which is 255. The principle of encoding uses the Least Significant Bit of each of these bytes, the bit on the far right side. If data is encoded to only the last two significant bits (which are the first and second LSB) of each color component it is most likely not going to be detectable; the human retina becomes the limiting factor in viewing pictures [7]. For the sake of this example only the least significant bit of each pixel will be used for embedding information. If the pixel value is 138 which is the value 10000110 in binary and the watermark bit is 1, the value of the pixel will be 10000111 in binary which is 139 in decimal. In this example we change the underline pixel.

III. Medical Image Watermarking

Medical image watermarking systems can be broken into three broad categories: robust, fragile, and semi-fragile. This section explains these terms and provides a brief review of existing systems in each category. Robust watermarks are designed to resist attempts to remove or destroy the watermark [1]. They are used primarily for copyright protection and content tracking. Many traditional robust methods are spread-spectrum, whereby the watermark is spread over a wide range of image frequencies [2]. More recent work includes the creation of image adaptive watermarks, where parameters change depending on local image characteristics. A number of robust medical image watermarking systems have been developed. For example one system uses a spread spectrum technique to encode copyright and patient information in images [4]. Another embeds a watermark in a spiral fashion around the Region of Interest (ROI) of an image [5].

Fragile watermarks are used to determine whether an image has been tampered with or modified [6, 7]. The watermark is destroyed if the image is manipulated in the slightest manner. Fragile watermarks are often capable of localization, and are used to determine where modifications were made to an image. Traditional methods embed checksums or pseudo-random sequences in the Least Significant Bit (LSB) plane. More recent work has employed increasingly sophisticated embedding techniques such as cryptographic hash functions.

Semi-fragile watermarks combine the properties of both robust and fragile watermarks. Like robust methods, they can tolerate some degree of change to the watermarked image (for example, quantisation noise from lossy compression). Like fragile methods, they are capable of localizing regions of an image that are authentic and those that have been altered. Recent work in the area includes embedding a heavily quantised version of the original image in the image, embedding key-dependent random patterns in blocks of the image, wavelet embedding, and embedding multiple watermarks.

IV. Some Definitions

Canny Edge Detector

The Canny edge detector is an edge detection operator that uses a multi-stage algorithm to detect a wide range of edges in images. An edge in an image may point in a variety of directions, so the Canny algorithm uses four filters to detect horizontal, vertical and diagonal edges in the blurred image. The edge detection operator returns a value for the first derivative in the horizontal direction (G_x) and the vertical direction (G_y). The edge gradient and direction can be determined from Eq.1. and Eq.2. respectively.

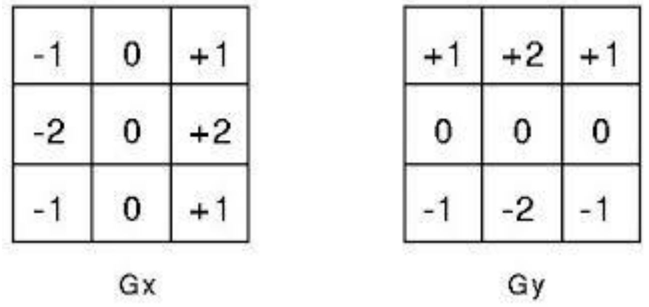
$$G = \sqrt{{G_x}^2 + {G_y}^2} \qquad (1)$$

$$\Theta=\text{atan2}\ (G_y, G_x) \qquad (2)$$

Where G can be computed using the hypot function and atan2 is the arc tangent function with two arguments. The edge direction angle is rounded to one of four angles representing vertical, horizontal and the two diagonals (0, 45, 90 and 135 degrees for example).

Sobel Edge Detector

The Sobel operator performs a 2-D spatial gradient measurement on an image and so emphasizes regions of high spatial frequency that correspond to edges. Typically it is used to find the approximate absolute gradient magnitude at each point in an input gray scale image.



-1	0	+1
-2	0	+2
-1	0	+1

Gx

+1	+2	+1
0	0	0
-1	-2	-1

Gy

Fig.2. Sobel Operator

The performance measures used in this paper provide some quantitative comparison among different edge detection schemes, mainly aiming at hybridization edge detection method comparison and measurement.

Mean Squared Error (MSE):

Mean Squared Error (MSE) gives an indication of how much degradation was introduced at a pixel based level. Higher the value of MSE, greater will be the level of degradation. Given a noise-free m×n monochrome image I and its noisy approximation K, MSE is defined as Eq.3.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \qquad (3)$$

Peak Signal to Noise Ratio (PSNR):

Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression). PSNR value can be determined by Eq.4.

$$\begin{aligned} PSNR &= 10.\log_{10}\frac{(MAX_I^2)}{(MSE)} \\ &= 20.\log_{10}(MAX_I) - 10.\log_{10}(MSE) \qquad (4) \end{aligned}$$

Signal to Noise Ratio (SNR):

SNR stands for signal to noise ratio. SNR value can be determined by Eq.5.

SNR= 20log10 (255/RMSE) (5)

Where RMSE means root mean square error.

V. METHODOLOGY

In this paper, the breast area will be identified first before the process of watermarking. The input is a mammogram image and patient's information. Identifying breast area will be done before the embedding process. So we use different type of edge detection method to identify the breast boundary. Now we will embed patient’s textual information with the mammogram image. After that, extracting process will be executed and finally, the output will be a watermarked mammogram images. Extracting process is a process that can extract the patient's information on watermarked image. Based on the result, all information that has been embedded in the samples of mammogram images can be read back without any interruption or data lost, this shows that the algorithm has successfully extracted the data and enables to authenticate the mammogram image. Figure 3 shows the idea of the proposed methodology.

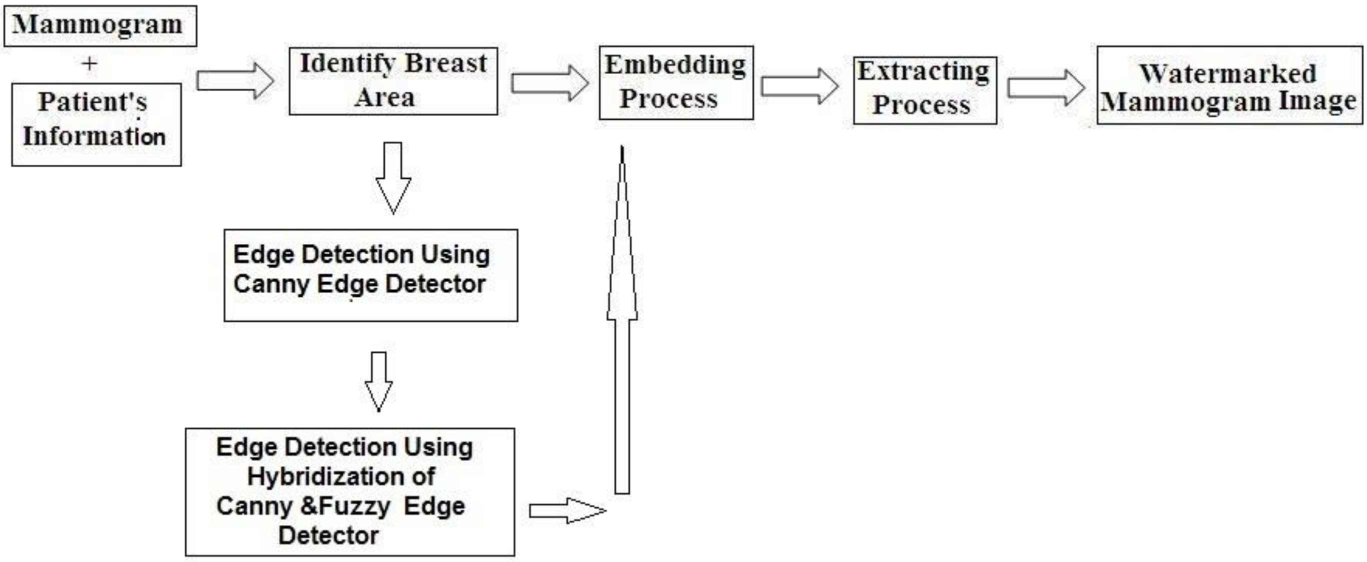

Mammogram
+
Patient's Information
Identify Breast Area
Embedding Process
Extracting Process
Watermarked Mammogram Image
Edge Detection Using Canny Edge Detector
Edge Detection Using Hybridization of Canny &Fuzzy Edge Detector

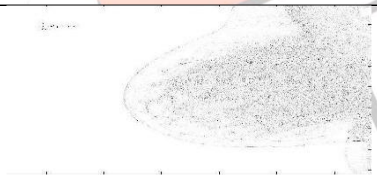
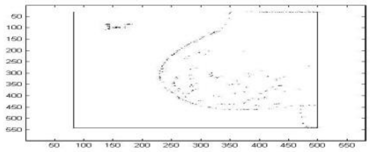
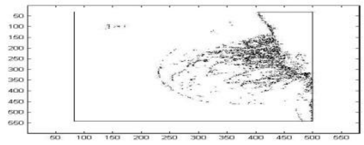
Fig.3. Block Diagram of the Proposed Methodology

Algorithm for the Edge Detection Using Hybridization [15]

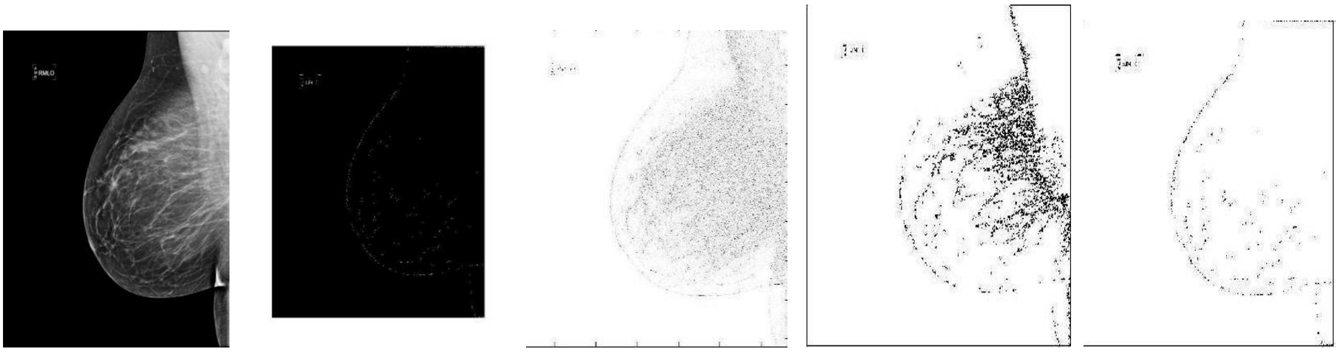
Step 1: Convolve image $f(r,c)$ with a Gaussian function to get smooth image $f(r,c)$.
Step 2: Apply first difference gradient operator to compute edge strength then edge magnitude and direction are obtained.
Step 3: Apply non-maximal or critical suppression to the gradient magnitude.
Step 4: Apply threshold to the non-maximal suppression.
Step 5: Obtain Image Gradient and Define Fuzzy Inference System (FIS) for edge detection.
Step 6: Specify FIS rules and Evaluate FIS on the image.

VI. COMPARISON BETWEEN DIFFERENT EDGE DETECTION TECHNIQUE

Table 1
Table for Analysis of the Performance of Different Edge Detection Technique

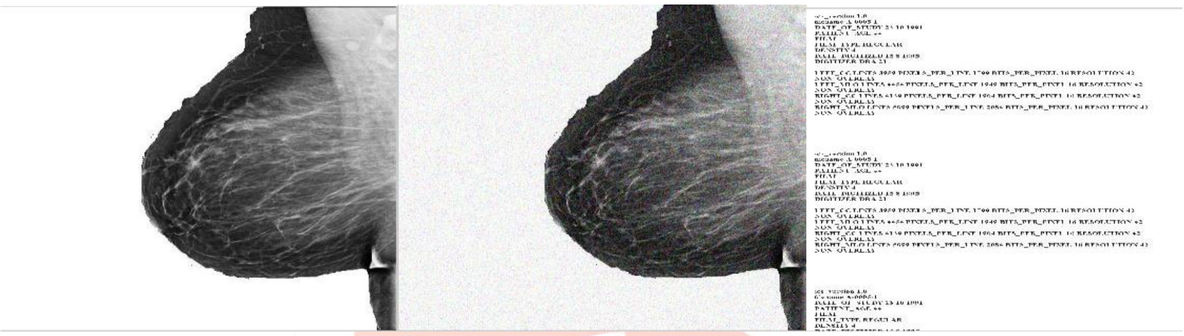
EDGE DETECTOR	***IMAGE***	***MSE***	***PSNR***	***SNR***
FUZZY		7.2241e+003	4.8057	-1.6918
CANNY FUZZY		7.1041e+003	4.8785	-1.6724
SOBEL FUZZY		7.3618e+003	4.7238	-1.6535

VII. Output of the Proposed Methodology



(a) (b) (c) (d) (e)

Fig.4. Result of Edge Detection (a) Input Image (b) Canny Edge Detection (c) Fuzzy Edge Detection (d) Hybrid: Sobel Fuzzy (e) Hybrid: Canny Fuzzy



```
ics_version 1.0
filename A-0005-1
DATE_OF_STUDY 25 10 1991
PATIENT_AGE 44
FILM
FILM_TYPE REGULAR
DENSITY 4
DATE_DIGITIZED 15 8 1995
DIGITIZER DBA 21

LEFT_CC LINES 3959 PIXELS_PER_LINE 1799 BITS_PER_PIXEL 16 RESOLUTION 42
NON_OVERLAY
LEFT_MLO LINES 4464 PIXELS_PER_LINE 1949 BITS_PER_PIXEL 16 RESOLUTION 42
NON_OVERLAY
RIGHT_CC LINES 4159 PIXELS_PER_LINE 1904 BITS_PER_PIXEL 16 RESOLUTION 42
NON_OVERLAY
RIGHT_MLO LINES 4699 PIXELS_PER_LINE 2056 BITS_PER_PIXEL 16 RESOLUTION 42
NON_OVERLAY

ics_version 1.0
filename A-0005-1
DATE_OF_STUDY 25 10 1991
PATIENT_AGE 44
FILM
FILM_TYPE REGULAR
DENSITY 4
DATE_DIGITIZED 15 8 1995
DIGITIZER DBA 21

LEFT_CC LINES 3959 PIXELS_PER_LINE 1799 BITS_PER_PIXEL 16 RESOLUTION 42
NON_OVERLAY
LEFT_MLO LINES 4464 PIXELS_PER_LINE 1949 BITS_PER_PIXEL 16 RESOLUTION 42
NON_OVERLAY
RIGHT_CC LINES 4159 PIXELS_PER_LINE 1904 BITS_PER_PIXEL 16 RESOLUTION 42
NON_OVERLAY
RIGHT_MLO LINES 4699 PIXELS_PER_LINE 2056 BITS_PER_PIXEL 16 RESOLUTION 42
NON_OVERLAY

ics_version 1.0
filename A-0005-1
DATE_OF_STUDY 25 10 1991
PATIENT_AGE 44
FILM
FILM_TYPE REGULAR
DENSITY 4
```

(a) (b) (c)

Fig.5. Result of Watermarking (a) Watermarked Image (hybrid of fuzzy and canny edge detection) (b) Watermarked with noised Image(c) Recovered Watermarked Image (Patient's Information)

VIII. Conclusion

A simple technique for digital mammogram authentication technique has been done here. Here, Image Watermarking using LSB technique has been used for embedding the message into the mammogram images. In this paper, better algorithm has been proposed to improve the detection of edges (breast boundary) by using hybrid edge detection rules. This is to differentiate the breast and background area of the mammogram images. The system begins to check the image authentication, which will help the hospitals to manage the huge medical information.

References

[1] E. T. Lin, C. I. Podilchuk, E. J. Delp," Detection of image alterations using semi-fragile watermarks", In Proc. of the SPIE Int. Conf. on Security and Watermarking of Multimedia Contents II, volume 3971, pages 152–163, San Jose, CA, USA, Jan. 2000.

[2] N. F. Johnson, Z. Duric, S. Jajodia, "Information Hiding: Steganograph and Watermarking - Attacks and Countermeasures", Kluwer Academic Press, Dordrecht, the Netherlands, 2001.

[3] Chang-Tsun Li, Yue Li, Chia-Hung Wei, "Protection of Digital Mammograms on PACSs Using Data Hiding Techniques", Department of Computer Science, University of Warwick, UK

[4] H. Tachibana, H. Harauchi, T. Ikeda, Y. Iwata, A. Takemura, T. Umeda, "Practical use of new watermarking and vpntechniques for medical image communication and archive", RSNA 2002 Archive, 2002, accessed 4 January 2005.

[5] A.Wakatani, "Digital watermarking for ROI medical images by using compressed signature image", In Annual Hawaii Int.Conf. on System Sciences, pages 2043– 2048, Hawaii, USA, Jan. 2002.

[6] J. Fridrich, M. Goljan, R. Du," Security and Watermarking of Multimedia Contents", In Proc. SPIE volume 3971, pages 197–208, San Jose, USA, Jan. 2001.

[7] B. Macq, F. Dewey,"Trusted headers for medical images", In DFG VIII-D II Watermarking Workshop, Erlangen, Germany, Oct. 1999.

[8] Deepshikha Chopra, Preeti Gupta, Gaur Sanjay B.C., Anil Gupta, "Lsb Based Digital Image Watermarking For Gray Scale Image", IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278- 0661, ISBN: 2278-8727 Volume 6, Issue 1 (Sep-Oct. 2012), PP 36-41

[9] Mohamed Ali Hajjaji, Abdellatif Mtibaa, El-beyBourennane, “A Watermarking of Medical Image: Method Based "LSB"”, Journal of Emerging Trends in Computing and Information Sciences, VOL. 2, NO.12, December 2011

[10] H. Ouahi, M. El Hajji, K. Afdel, “Secure and Image Retrieval based on Multipurpose Watermarking for Mammography Images Database”, International Journal of Computer Applications (0975 – 8887) Volume 90 – No 14, March 2014

[11] Y.I. Khamlichi, M. Machkour, K. Afdel, A. Moudden, “Medical Image Watermarked by Simultaneous Moment Invariants and Content-Based for Privacy and Tamper Detection”, Proceedings of the 6th WSEAS International Conference on Multimedia Systems & Signal Processing, Hangzhou, China, April 16-18, 2006 (pp109-113)

[12] M. L. D. Wong, S. I. J. Lau, N. S. Chong, and K. Y. Sim, “A Salient Region Watermarking Scheme for Digital Mammogram Authentication”, International Journal of Innovation, Management and Technology, Vol. 4, No. 2, April 2013

[13] S. Boucherkha, M. Benmohamed. "A Lossless Watermarking Based Authentication System for Medical Images", Proceedings of World Academy of Science, Engineering and Technology. Page: 100- 103, 2005.

[14] Azizah A. Manaf, Akram M. Zeki, CikFeresa M Foozy, ”Digital Watermarking For Mammogram Authentication”, International Conference on Fundamental and Applied (Icfas), 15-17 June 2010 Kuala Lumpur Convention Centre.

[15] Samya Muhuri, “Digital Watermarking for Mammogram Authentication Technique”, International Journal of Research in Information Technology, Volume 2, Issue 6, June 2014, Pg: 15-21